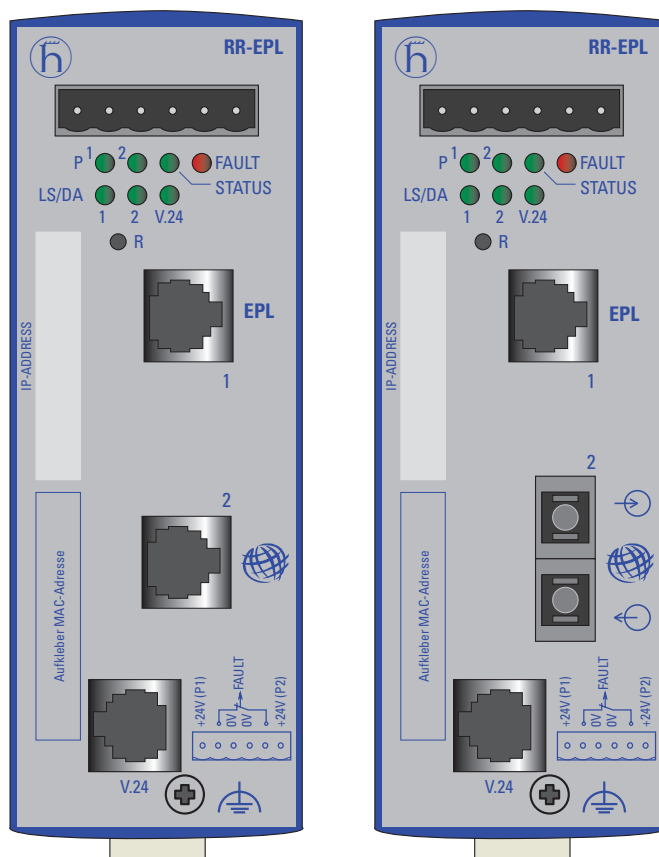


User Manual

Management

Industrial ETHERNET Rail Router ETHERNET Powerlink RR-EPL TX/TX, RR-EPL TX/MM SC



The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

© 2006 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use.

The performance features described here are binding only if they have been expressly guaranteed in the contract. This publication has been created by Hirschmann Automation and Control GmbH according to the best of our knowledge. Hirschmann reserves the right to change the contents of this manual without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the details in this publication.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

Printed in Germany (1.2.06)

Hirschmann Automation and Control GmbH
Stuttgarter Straße 45-51
72654 Neckartenzlingen
Tel. +49 1805 141538

039 506-001-01-0106

Content

	Safety instructions	7
1	Introduction	13
1.1	Requirement and solution	14
1.2	Product features	16
1.3	Device models	18
2	Typical application scenarios	19
3	Hardware	23
3.1	Display	24
	3.1.1 Device status	24
	3.1.2 Port status	26
	3.1.3 Function state	26
3.2	Recovery button	27
4	Installation and startup procedure	29
4.1	Device installation	30
	4.1.1 6-pin terminal block	30
	4.1.2 Assembly	31
	4.1.3 Interfaces	33
	4.1.4 Disassembly	36
4.2	Startup operation	37
4.3	Basic settings	38
	4.3.1 System configuration via HiDiscovery	39
	4.3.2 System configuration via V.24	40

5	Configuration	41
5.1	Setting up a local configuration connection	42
5.1.1	Web-based administrator interface	42
5.1.2	After a successful connection setup	44
5.2	Remote configuration	47
5.2.1	Remote configuration via LAN	47
5.2.2	Remote configuration via modem	48
6	Web-based management	53
6.1	Overview	54
6.2	System menu	55
6.2.1	System:Configurations-Profiles	55
6.2.2	System:Configuration Pull	58
6.2.3	System:Reboot	59
6.2.4	System:Logs - Display	60
6.2.5	System:HiDiscovery	61
6.2.6	System:Signal contact	62
6.3	Ports menu	64
6.3.1	Ports:Configuration Table	64
6.4	Ethernet Powerlink menu	66
6.4.1	Ethernet Powerlink:Setup	66
6.4.2	Ethernet Powerlink:Reset	68
6.4.3	Ethernet Powerlink:SDO Access	68
6.4.4	Protecting the EPL segment	71
6.4.5	Ethernet Powerlink:Logs - Display	71
6.5	Network menu	72
6.5.1	Network:Base	72
6.5.2	Network:Router	76
6.5.3	Network:PPPoE	78
6.5.4	Network:PPTP	79
6.5.5	Network:Extended Settings	81
6.5.6	Network:Status	82
6.6	Configuring the firewall	83
6.6.1	Firewall:Incoming	84
6.6.2	Firewall:Outgoing	86
6.6.3	Firewall:Port Forwarding	88
6.6.4	Firewall:NAT	90

6.6.5	Firewall:1-to-1 NAT	93
6.6.6	Firewall:Extended Settings	95
6.6.7	Firewall:Logs - Display	96
6.7	Setting up a VPN connection	97
6.7.1	VPN:Connections	98
6.7.2	VPN:Machine Certificate	111
6.7.3	VPN:L2TP	114
6.7.4	VPN Configuration, IPsec Status - Display	115
6.7.5	VPN:L2TP Status - Display	116
6.7.6	VPN:VPN Logs - Display	116
6.8	Services menu	117
6.8.1	Services:DNS	117
6.8.2	Services:DynDNS Monitoring	120
6.8.3	Services:DynDNS registration	121
6.8.4	Services:DHCP Intern (trusted port)	123
6.8.5	Services:DHCP Extern (untrusted port)	125
6.8.6	Services:LLDP	128
6.8.7	Services:NTP	129
6.8.8	Services:Remote Logging	131
6.8.9	Services:SNMP Traps	133
6.9	Access menu	136
6.9.1	Access:passwords	136
6.9.2	Access:Language	138
6.9.3	Access:HTTPS	139
6.9.4	Access:SSH	142
6.9.5	Access:SNMP	145
6.9.6	Access:Serial Port/Modem	148
6.10	Features menu	151
6.10.1	Features:Local Update	151
6.10.2	Features:Online Update	152
6.10.3	Features:Software Information - Display	154
6.10.4	Features:Hardware information	155
6.11	Support menu	156
6.11.1	Support:Snapshot	156
6.11.2	Support:Status - Display	157
6.12	CIDR (Classless InterDomain Routing)	160
6.13	Example of a network	162

7	The Recovery button	165
7.1	Performing a restart	166
7.2	Executing the recovery procedure	167
	7.2.1 Aim	167
	7.2.2 Action	167
7.3	Flashing the firmware	168
	7.3.1 Requirements for flashing the firmware	170
	7.3.2 Installing the DHCP and tftp server under Windows	171
	7.3.3 Installing DHCP and TFTP servers under Linux	173
8	HiConfig	175
A	Appendix	183
A.1	FAQ	184
A.2	Based specifications and standards	185
A.3	SNMP traps	187
A.4	Certifications	189
A.5	Technical data	190
A.6	Copyright of integrated software	194
B	Glossar	195
C	Reader's comments	203
D	Index	205
	Hirschmann Competence	209

Safety instructions

■ **Supply voltage**

The devices are designed for operation with a safety extra-low voltage. They may only be connected to the supply voltage connections and to the signal contact with PELV circuits or alternatively SELV circuits with the voltage restrictions in accordance with IEC/EN 60950.

The supply voltage is electrically isolated from the housing.

☐ Never start operation with damaged components!

☐ Relevant for North America:

The subject unit is to be supplied by a Class 2 power source complying with the requirements of the National Electrical Code, table 11(b). If power is redundant supplied (two individual power sources) the power sources together should comply with the requirements of the National Electrical Code, table 11 (b).

☐ Relevant for North America:

Use 60/75°C or 75°C copper(CU)wire only.

☐ Relevant für Nordamerika:

Power, input and output (I/O) wiring must be in accordance with Class I, Division 2 wiring methods [Article 501-4(b) of the National Electrical Code, NFPA 70] and in accordance with the authority having jurisdiction.

■ **Shielding ground**

The shielding ground of the connectable twisted pair lines is connected to the front panel as a conductor.

☐ Beware of possible short circuits when connecting a cable section with conductive shielding braiding.

■ **Housing**

Only technicians authorized by Hirschmann are permitted to open the housing.

The device is grounded via the separated ground screw. It is located on the bottom of the front panel.

- ☐ Make sure that the electrical installation meets local or nationally applicable safety regulations.
- ☐ The ventilation slits must not be covered to ensure free air circulation.
- ☐ The distance to the ventilation slots of the housing has to be a minimum of 10 cm.
- ☐ Never insert pointed objects (thin screwdrivers, wires, etc.) into the inside of the subrack! Failure to observe this point may result in injuries caused by electric shocks.
- ☐ The housing has to be mounted in upright position.
- ☐ If installed in a living area or office environment, the device must be operated exclusively in switch cabinets with fire protection characteristics according to EN 60950.

■ **Environment**

The device may only be operated in the listed maximum surrounding air temperature range at the listed relative air humidity range (non-condensing).

- ☐ The installation location is to be selected so as to ensure compliance with the climatic limits listed in the Technical Data.
- ☐ To be used in a Pollution Degree 2 environment only.

■ **Qualification requirements for personnel**

Qualified personnel as understood in this manual and the warning signs, are persons who are familiar with the setup, assembly, startup, and operation of this product and are appropriately qualified for their job. This includes, for example, those persons who have been:

- ▶ trained or directed or authorized to switch on and off, to ground and to label power circuits and devices or systems in accordance with current safety engineering standards;
- ▶ trained or directed in the care and use of appropriate safety equipment in accordance with the current standards of safety engineering;
- ▶ trained in providing first aid.

■ **General Safety Instructions**

This device is electrically operated. Adhere strictly to the safety requirements relating to voltages applied to the device as described in the operating instructions!

Failure to observe the information given in the warnings could result in serious injury and/or major damage.

- ☐ Only personnel that have received appropriate training should operate this device or work in its immediate vicinity. The personnel must be fully familiar with all of the warnings and maintenance measures in these operating instructions.
- ☐ Correct transport, storage, and assembly as well as careful operation and maintenance are essential in ensuring safe and reliable operation of this device.
- ☐ These products are only to be used in the manner indicated in this version of the manual.
- ☐ Any work that may have to be performed on the electrical installation should be performed by fully qualified technicians only.

Warning!

LED- or LASER components according to IEC 60825-1 (2001):
CLASS 1 LASER PRODUCT.
LIGHT EMITTING DIODE - CLASS 1 LED PRODUCT.

■ **National and international safety regulations**

- ☐ Make sure that the electrical installation meets local or nationally applicable safety regulations.

■ **Note on the CE marking**

The devices comply with the regulations contained in the following European directives:

89/336/EEC

Directive of the council for standardizing the regulations of member states on electromagnetic compatibility (changed by RL 91/263/EEC, 92/31/EEC and 93/68/EEC).

In accordance with the above-named EU directives, the EU conformity declaration will be at the disposal of the relevant authorities at the following address:

Hirschmann Automation and Control GmbH
Stuttgarter Straße 45-51
D-72654 Neckartenzlingen
Germany
Phone ++49 7127 14 1480

The product can be used in living areas (living area, place of business, small business) and in industrial areas.

- ▶ Interference immunity: EN 61000-6-2:2001
- ▶ Emitted interference: EN 55022:1998 + A1 2000 Class A

Warning!

This is a class A device. This device can cause interference in living areas, and in this case the operator may be required to take appropriate measures.

The assembly guidelines provided in these instructions must be strictly adhered to in order to observe the EMC value limits.

■ **FCC note:**

Appropriate testing has established that this device fulfills the requirements of a class A digital device in line with part 15 of the FCC regulations.

These requirements are designed to provide sufficient protection against interference where the device is being used in a business environment. The device creates and uses high frequencies and can radiate same, and if it is not installed and used in accordance with this operating manual, it can cause radio transmission interference. The use of this device in a living area can also cause interference, and in this case the user is obliged to cover the costs of removing the interference.

■ **Recycling note:**

After usage, this product must be disposed of properly as electronic waste in accordance with the current disposal regulations of your county / state / country.

1 Introduction

Today, Ethernet is the most widely used type of communications technology. It has become the de facto standard in an office environment. Ethernet technology is also gaining significance in the field of industrial automation. In addition to the advantages of using a standardized form of communication, Ethernet allows for a seamless infrastructure that extends from the office all the way to the machine or sensor. Consequently, not only are process and production data available on the field level, but they also integrate seamlessly with interdepartmental data acquisition systems. Despite these advantages there are new issues that must be solved to be able to operate the installations securely and reliably. A top-priority issue is that of security which is determined by the factors: authentication, authorization, confidentiality, availability and data integrity.

1.1 Requirement and solution

Increasing standardization and networking in the field of automation will lead to increased vulnerability of these networks. The threat emanates from dangers which office users have been exposed to for quite some time and which they have been attempting to ward off with popular security solutions -- with mixed success.

The greatest danger is not only from hackers and is often not intentional. Fusing the office and production network makes for easy prey when it comes to the risks posed by worms. Furthermore, machine and production cells are often unprotected against intrusions (for example, faulty addressing or faulty program code) from the production network.

Today this no longer has to be the case:

The industrial firewall and virtual private network (VPN) system RR-EPL monitors with an "eagle's eye" the security of networks across company borders. The RR-EPL provides secure access to a real-time ETHERNET Powerlink network segment. It also supports the ETHERNET Powerlink protocol V2.0 at the EPL port. The RR-EPL works as a Controlled Node (CN) and performs the tasks of a type 1 ETHERNET Powerlink router.

Migration is performed in existing networks for secure and insecure ports via twisted pair and F/O connections. Furthermore, a V.24 port is available for configuration and for connecting a modem.

The scaleable security function featuring a

- ▶ Pure firewall or a
 - ▶ Firewall and VPN function
- provides customized protection.

In router mode, subnetworks can be separated from the main network. You can use the simple 1-to-1 NAT or NAT configuration and the stateful inspection firewall to realize secure access protection on different ETHERNET Powerlink segments in the factory network.

The integrated DHCP server makes it easy and safe to set up service ports for employees in the field.

By providing a login procedure (internal and external), it is possible to analyze and thus optimize the data traffic.

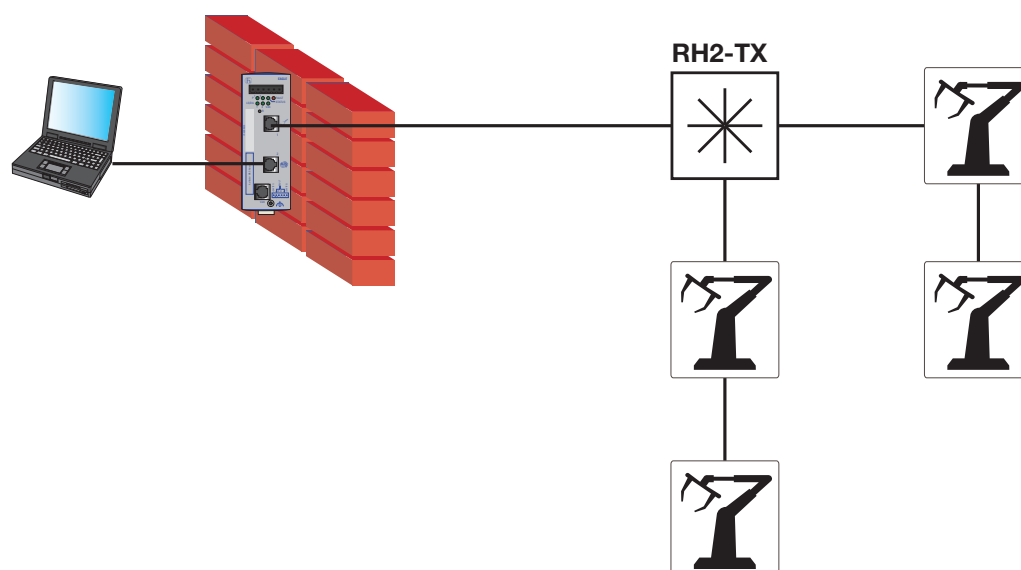


Fig. 1: A typical application scenario (for further application scenarios, see [Page 19](#))

1.2 Product features

The state-of-the-art security system secures the authentication, fuse protection, and confidentiality of the communication in production networks: In combination with the RR-EPL, firewalls, VPNs and scaleable security functions provide the highest possible level of protection for industrial networks and prevent inadvertent and uncontrolled data manipulation.

- ▶ Scalability of the security function:
 - pure firewall
 - firewall with VPN function
- ▶ Creation of subnetworks:
 - router mode
- ▶ The router mode and the 1-to-1 NAT or NAT allow access to different similarly structured EPL segments.
- ▶ Easy starting operation:
 - HiDiscovery support
 - support for the AutoConfiguration adapter
- ▶ Remote access to the network:
 - dial-in access via V.24
- ▶ Extensive diagnostics:
 - Web-based management
 - status LEDs
 - signal contact
 - logging in to the SysLog server
 - integration with HiVision
- ▶ Migration to existing networks:
 - Twisted pair and F/O links for secure port
- ▶ Design suitable for industrial use:
 - redundant 24 V power supply
 - can be mounted to a top-hat rail
 - IP 20 without fan
- ▶ VLAN
- ▶ MAC filter rules
- ▶ 1-to-1 NAT
- ▶ Sortable firewall rules

- ▶ LLDP (802.1AB)
- ▶ DHCP Relay and Option 82

1.3 Device models

The RR-EPL is available in 2 different models:

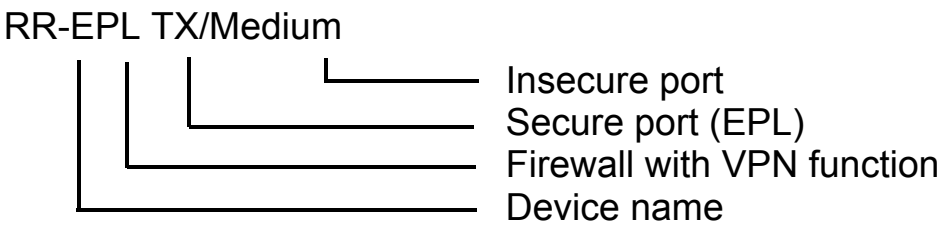


Fig. 2: Device identifier:

Device type	TP ports 10/100	F/O port multimode 100 MBit/s
RR-EPL TX/TX	2	
RR-EPL TX/MM SC	1	1

Table 1: Device models

2 Typical application scenarios

The most common applications used in industry require the operation of the RR-EPL in Router mode.

■ Remote access via a VPN tunnel

A dedicated VPN client software program must be running on the single computer. Windows 2000/XP contains the VPN client software.

Network mode of the RR-EPL: router

- ▶ In router mode, the RR-EPL must be defined as the standard gateway on the locally connected client computer.

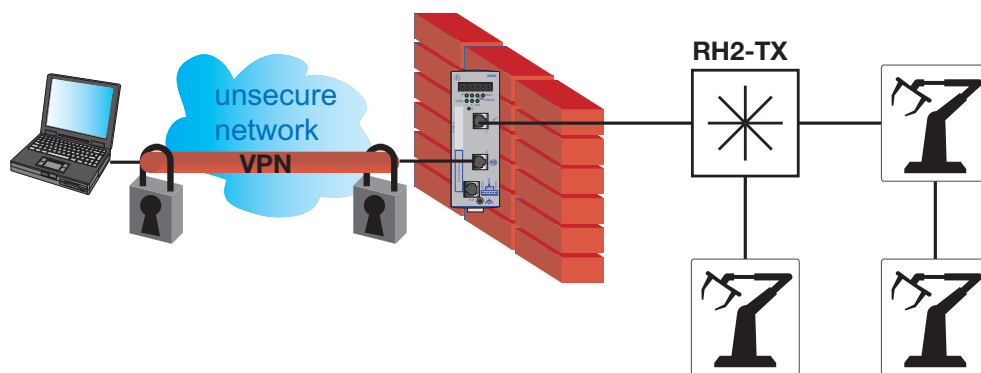


Fig. 3: Example of remote access via a VPN tunnel

■ Secure cell separation

Network mode of the RR-EPL: Router mode

- ▶ In router mode, the RR-EPL must be defined as the standard gateway on the client computer connected to the secure port.
- ▶ 1-to-1 NAT or NAT
- ▶ Appropriate 1-to-1 NAT or NAT entries allow access to different EPL cells.
- ▶ You can easily configure the access protection using firewall entries.

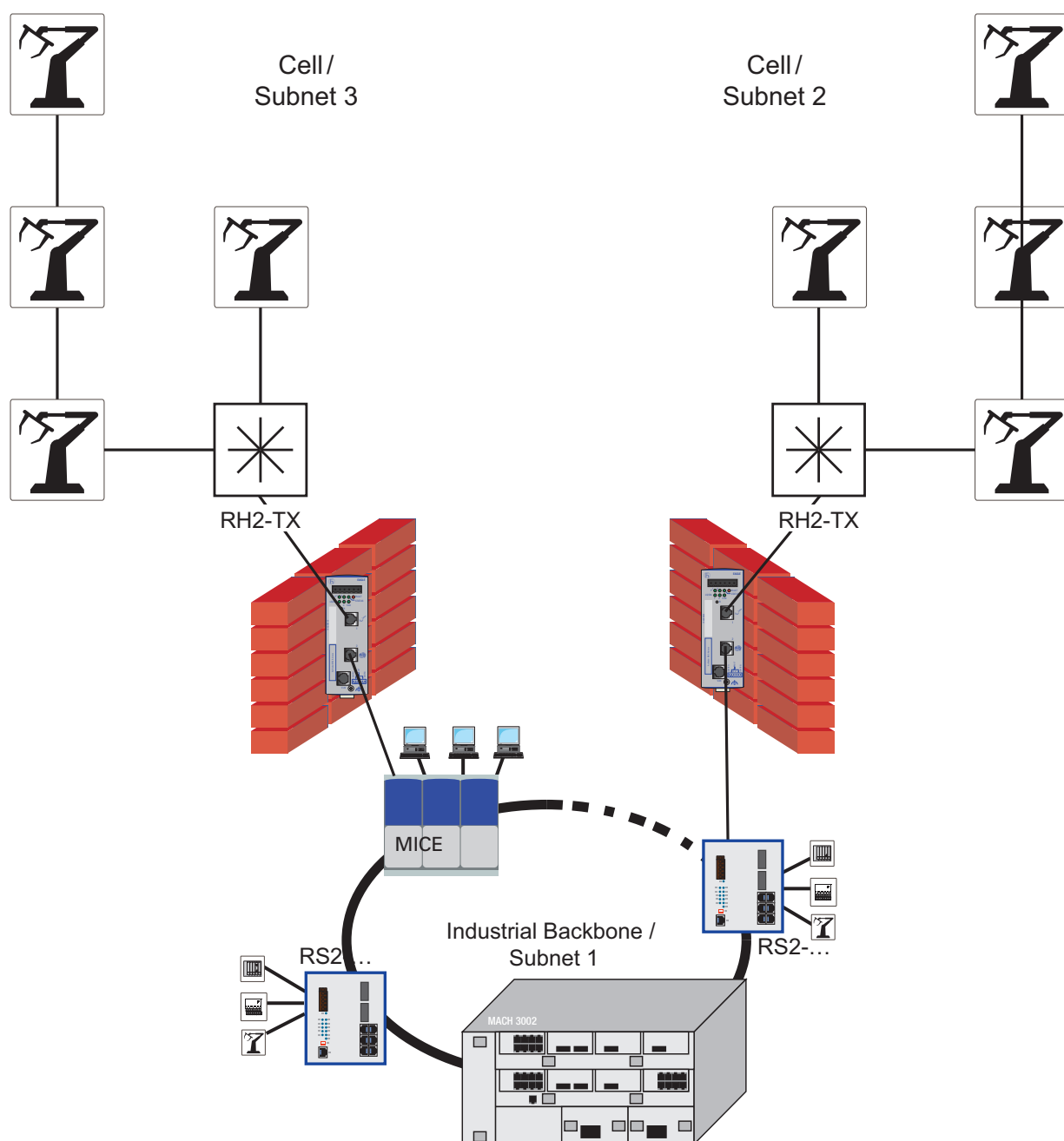


Fig. 4: Example of secure cell separation

■ Secure service port

Network mode of the RR-EPL: router mode.

- ▶ In router mode, the RR-EPL must be defined as the standard gateway on the client computer connected to the secure port.
- ▶ Configuration of the RR-EPL as the DHCP server: on the insecure port, enter the MAC-IP allocation ([see Fig. 61](#)).
- ▶ Definition of firewall rules for the IP address entered in the DHCP server.

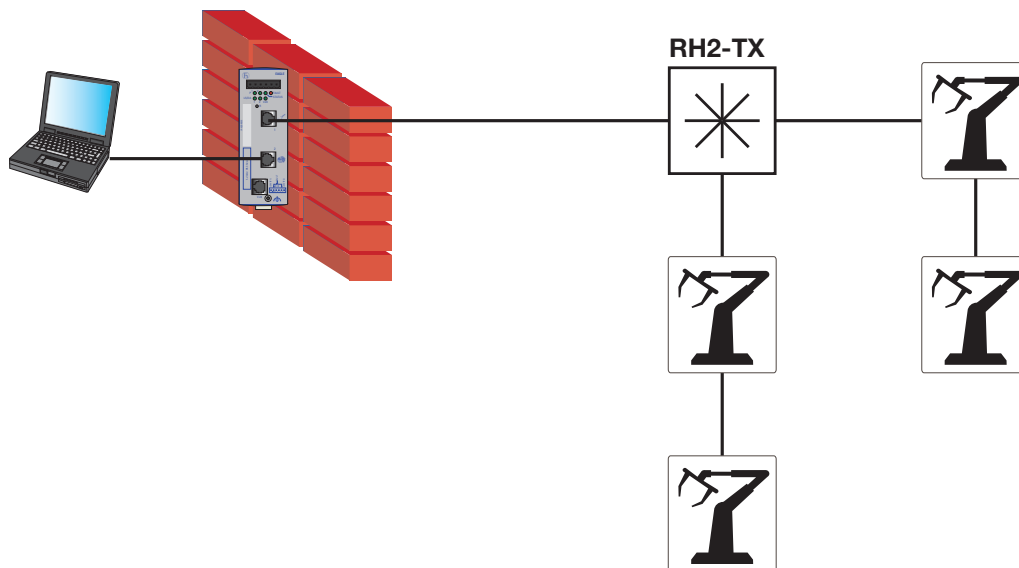


Fig. 5: Example of a secure service port

■ **Secure connection of networks**

Network mode of the RR-EPL: Router

- ▶ In router mode, the RR-EPL must be defined as the standard gateway on the client computer connected to the secure port.
- ▶ If you use a DSL modem, make the PPPoE settings (see [“Network:PPPoE” on page 78](#)).

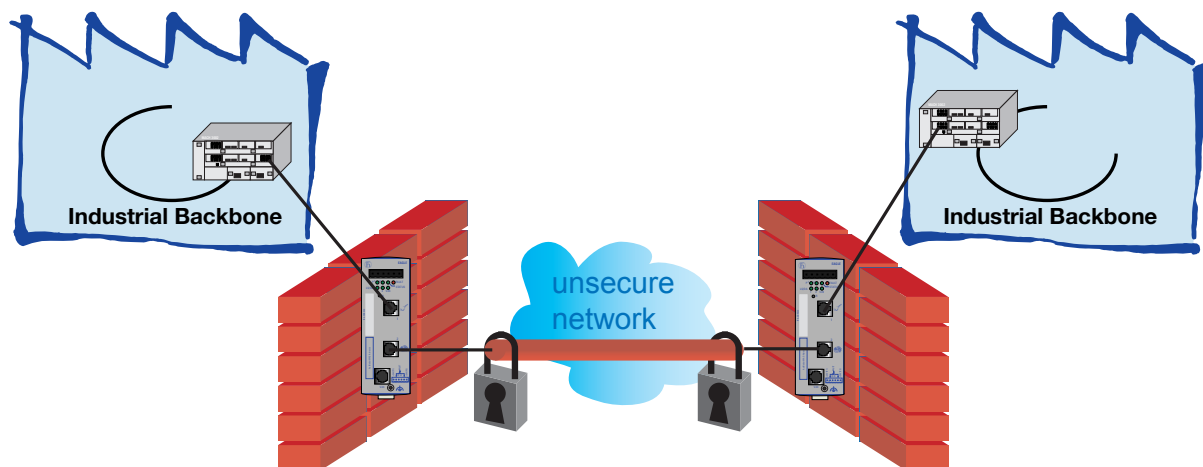


Fig. 6: Example of a secure connection of networks

3 Hardware

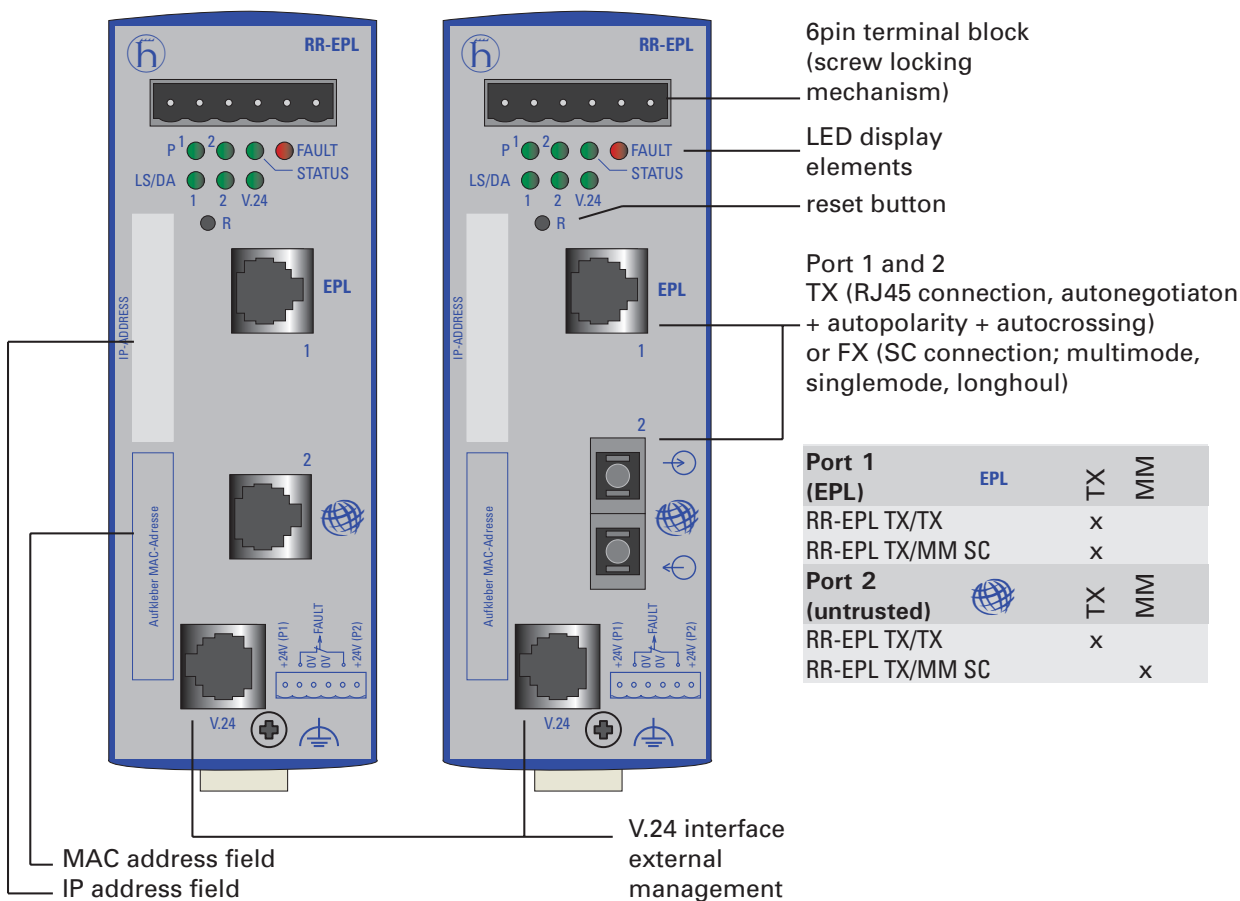


Fig. 7: Front view

3.1 Display

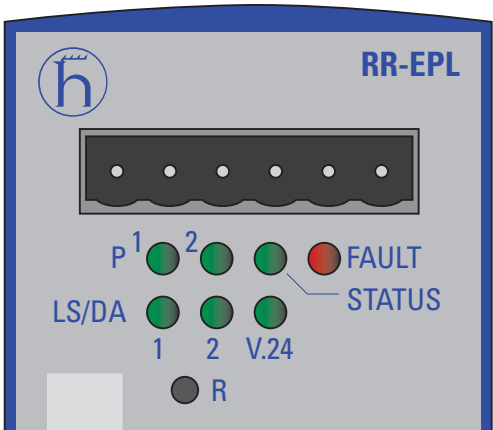


Fig. 8: Display

3.1.1 Device status

These LEDs provide information about statuses which affect the function of the entire RR-EPL.

■ P1 - Power 1 (Green LED)

Display	Meaning
lit	Supply voltage 1 is present.
not lit	Supply voltage 1 is less than 9.6 V.

■ P2 - Power 2 (Green LED)

Display	Meaning
lit	Supply voltage 2 is present.
not lit	Supply voltage 2 is less than 9.6 V.

■ FAULT - Failure (Red LED)

Display	Meaning
lit	The indicator contact is open, i.e. incorrect EPL status.
not lit	The indicator contact is closed, i.e. EPL without error.

If the “Operational supervision” on page 62 is active for the signal contact, then the error display is independant of the signal contact position.

■ STATUS - Device status (Yellow/green LED)

Display	Meaning
flashes green	Initialization of the device.
not lit	EPL not active.
flickers green	BASIC-ETHERNET mode
flashes once a second green	Managing node looking for subscribers.
flashes twice a second green	EPL subscribers found.
flashes three times a second green	EPL initialization complete.
lit green	EPL active.

■ AutoConfiguration Adapter ACA

The “STATUS” and “V.24” LEDs display memory operations of the ACA 11.

Display	Meaning
flashing alternatively:	Error in memory operation.
LEDs flash simultaneously; twice a second	Loading the configuration from the ACA.
LEDs flash simultaneously; once a second	Saving the configuration to the ACA.

3.1.2 Port status

These LEDs display port-related information.

■ **LS/DA 1, 2 and V.24 - Data, Link status (green/yellow LED)**

Display	Meaning
not lit	No valid link.
lit green	Valid link.
flashes yellow	Receiving data.
running light	Initialization phase after a reset.

3.1.3 Function state

These displays go together with the Recovery button (refer to [“The Recovery button” on page 165](#)).

3.2 Recovery button

The Recovery button is used to set the device into the following states:

- ▶ Restart (refer to [“Performing a restart” on page 166](#)),
- ▶ Recovery procedure (refer to [“Executing the recovery procedure” on page 167](#)),
- ▶ Flashing the firmware (refer to [“Flashing the firmware” on page 168](#))

4 Installation and startup procedure

The RR-EPL industrial firewall/VPN system has been developed for practical applications in a harsh industrial environment. Accordingly, the installation process has been kept simple. The few configuration settings required for operation are described in this chapter.

Note: For security reasons, change the root and the administrator passwords when you initially change the configuration.

4.1 Device installation

4.1.1 6-pin terminal block

The supply voltage and the signal contact are connected via a 6-pin terminal block with snap lock.

Warning!

The devices are designed for operation with safety extra-low voltage. Thus, they may only be connected to the supply voltage connections and to the signal contact with PELV circuits or alternatively SELV circuits with the voltage restrictions in accordance with IEC/EN 60950.

■ **Supply voltage**

The supply voltage can be connected redundantly. Both inputs are uncoupled. There is no distributed load. With redundant supply, the transformer supplies the device alone with the higher output voltage. The supply voltage is electrically isolated from the housing.

■ **Signal contact**

The signal contact monitors proper functioning of the device, thus enabling remote diagnostics.

A break in contact is reported via the potential-free signal contact (relay contact, closed circuit):

- ▶ The failure of at least one of the two supply voltages (supply voltage 1 or 2 < 9,6 V).
- ▶ A continuous malfunction in the device (internal 3.3 VDC voltage).
- ▶ The defective link status of at least one port. With the device the indication of link status can be masked by the management for each port. Link status is not monitored in the delivery condition.
- ▶ Error during self-test.

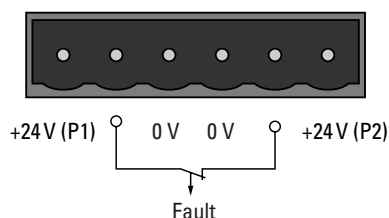


Fig. 9: Pin assignment of the 6-pin terminal block

- ☐ Pull the terminal block off the device and connect the power supply and signal lines.

4.1.2 Assembly

On delivery, the device is ready for operation.

- ☐ Attach the upper snap-in guide of the device into the top-hat rail and press it down against the top-hat rail until it snaps into place.

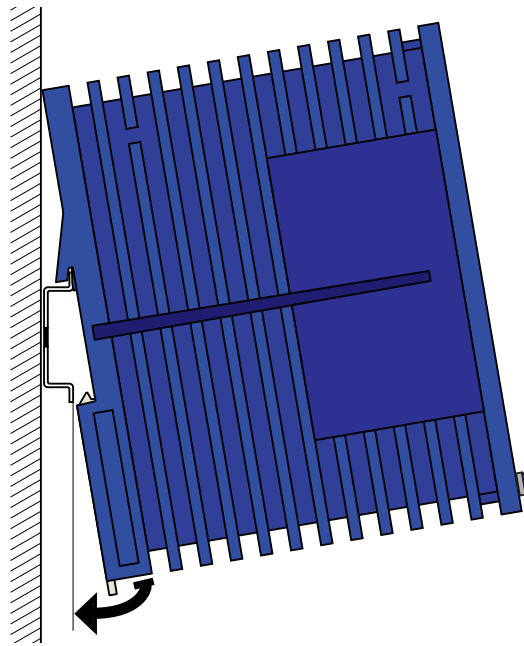


Fig. 10: Assembly

Note: The front panel of the housing is grounded via a ground connection.

Note: The housing must not be opened.

Note: The shielding ground of the industrial connectable twisted pair lines is connected to the front panel as a conductor.

4.1.3 Interfaces

■ 10/100 Mbit/s connection

10/100 Mbit/s ports (8-pin RJ45 socket) enable the connection of terminal devices or independent network segments in compliance with the IEEE 802.3 100BASE-TX / 10BASE-T standards. These ports support:

- ▶ auto-negotiation
- ▶ autocrossing (when autonegotiation is switched off)
- ▶ autopolarity
- ▶ 100 Mbit/s half duplex mode
- ▶ 100 Mbit/s full duplex mode
- ▶ 10 Mbit/s half duplex mode
- ▶ 10 Mbit/s full duplex mode

State on delivery: Autonegotiation activated. Alternative to the Web-based interface (see [“Ports:Configuration Table” on page 64](#)), the HiConfig interface (see [“HiConfig” on page 175](#)) allows you to change this setting. While you have access to the Web-based interface of the RR-EPL via the secure and insecure port, you can also reach the HiConfig interface via the V.24 port.

The socket housings are electrically connected to the front panel.

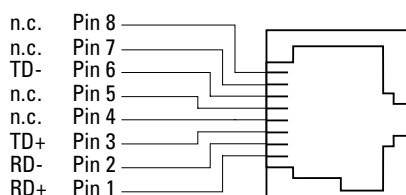


Fig. 11: Pin assignment of a TP/TX interface in MDI-X mode, RJ45 socket

■ 100 Mbit/s F/O connection

100 MBit/s F/O ports (DSC sockets) enable the connection of terminal devices or independent network segments in compliance with the IEEE 802.3 100BASE-FX standard. These ports support:

- ▶ full and half duplex mode.

State on delivery: full duplex. This configuration is required to form redundant structures.

■ V.24 interface (external management)

A serial interface is provided on the RJ11 socket (V.24 interface) for the local connection of

- ▶ an external management station (VT100 terminal or PC with appropriate terminal emulation).
- ▶ a modem (via PPP).
- ▶ an ACA 11 AutoConfiguration Adapter.

VT-100 terminal settings in state on delivery:

- Speed: 9,600 baud
- Data: 8 bit
- Stopbit: 1 bit
- Handshake: off
- Parity: none

The socket housing is electrically connected to the lower covering of the device.

The signal lines are electrically isolated from the supply voltage (60 V insulation voltage) and the front panel.

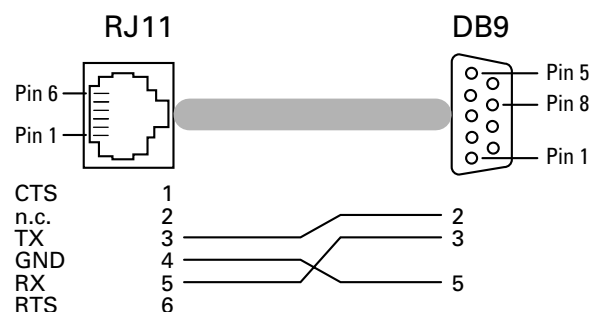


Fig. 12: Pin assignment of the terminal cable

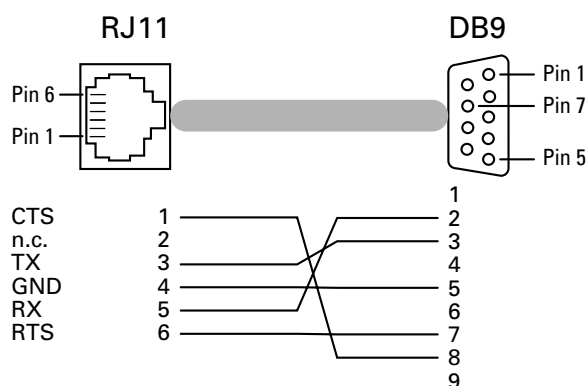


Fig. 13: Pin assignment of the modem cable

- ☐ Install the signal lines and, if necessary, the terminal/modem cable.
- ☐ Attach the ground cable to the ground screw.

4.1.4 Disassembly

- In order to remove the device from the top-hat rail, move the screwdriver horizontally under the chassis in the locking gate, pull this down — without tilting the screwdriver — and fold the device up.

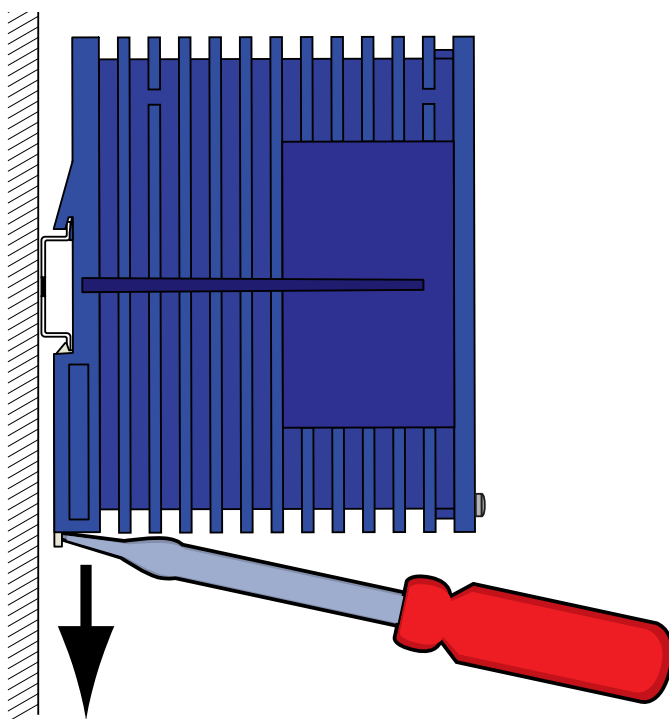


Fig. 14: Disassembly

4.2 Startup operation

When the supply voltage is connected via the terminal, start up the device.

4.3 Basic settings

In its state on delivery, the device operates as a type 1 ETHERNET Powerlink router. In the BASIC ETHERNET mode, the RR-EPL is accessed via the IP address 192.168.100.254 with the network mask 255.255.255.0 on the EPL port.

The firewall has been preconfigured so that all IP traffic from the secure network is possible and traffic from the insecure network to the secure one is possible.

The RR-EPL provides 4 options for configuring the IP address of the unsecure port:

- ▶ Entry by HiDiscovery protocol,
- ▶ Entry via the Web-based management (via EPL port),
- ▶ Entry via the V.24 port,
- ▶ DHCP.

4.3.1 System configuration via HiDiscovery

The HiDiscovery protocol enables you to assign IP parameters to the device via the unsecure network.

You can easily configure additional parameters with the [“Web-based management”](#) on page 53.

Install the HiDiscovery software on your PC. The software is on the CD supplied with the device.

- ☐ To install it, you start the installation program on the CD.

Note: The installation of HiDiscovery involves installing the WinPcap Version 3.0 software package.

If an earlier version of WinPcap is already installed on the PC, then you must first uninstall it. A newer version remains intact when you install HiDiscovery. However, this can not be guaranteed for all future versions of WinPcap. In the event that the installation of HiDiscovery has overwritten a newer version of WinPcap, then you uninstall WinPcap 3.0 and then re-install the new version.

- ☐ Start the HiDiscovery program.

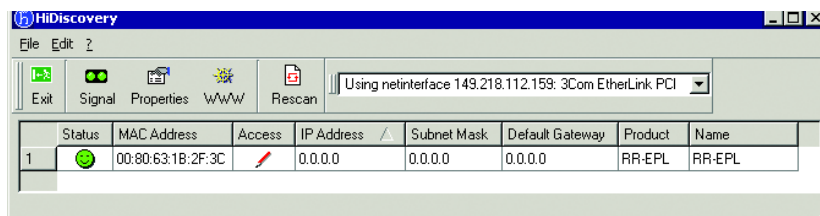


Fig. 15: HiDiscovery

When HiDiscovery is started, it automatically searches the network for those devices which support the HiDiscovery protocol.

HiDiscovery uses the first PC network card found. If your computer has several network cards, you can select these in HiDiscovery on the toolbar.

HiDiscovery enables you to identify the devices displayed.

- ☐ Select a device line.
- ☐ Click on the symbol with the two green dots in the tool bar to set the LEDs for the selected device flashing. To switch off the flashing, click on the symbol again.

By double-clicking a line, you open a window in which you can enter the device name and the IP parameter.

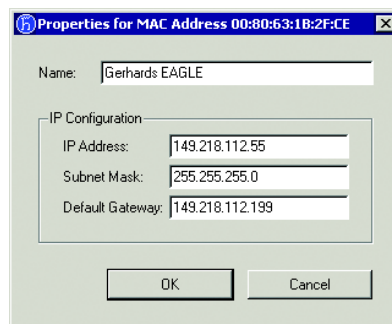


Fig. 16: HiDiscovery - assigning IP parameters

Note: For security reasons, switch off the HiDiscovery function for the device in the Web-based management, after you have assigned the IP parameters to the device.

4.3.2 System configuration via V.24

Connect your PC with the RR-EPL as described in [“Making a connection to HiConfig over a V.24 port.” on page 177.](#)

For entering IP parameters see [“IP parameter configuration in transparent mode” on page 181.](#)

5 Configuration

Requirements

- ▶ For local configuration:
The computer with which you make the configuration must be either
 - directly connected to the device,
 - or it must be connected to it via the local network.
- ▶ For remote configuration on the insecure port:
The RR-EPL must be configured in such a way that it allows remote configuration.
- ▶ The RR-EPL must be switched on, i.e. must be connected to a power supply unit so that it is supplied with current.
- ▶ The RR-EPL must be connected, i.e. the required connections must function properly.

5.1 Setting up a local configuration connection

5.1.1 Web-based administrator interface

The RR-EPL is configured with the Web browser that runs on the configuration computer (for example MS Internet-Explorer starting with version 5.0 or Netscape Communicator starting with version 4.0)

Hinweis: The Web browser must support SSL (i.e. https).

Depending on the network mode (operating mode) in which the RR-EPL is in, it can be reached at the one of the following addresses according to the factory setting:

Mode	Address
EPL	https://192.168.100.254/
unsecure port	https://IP address (see “Basic settings” on page 38)

Table 2: Address line of the browsers

Proceed as follows:

- ☐ Start a Web browser.
(For example, MS Internet Explorer Version 5.0 or later or Netscape Communicator Version 4.0 or later; the Web browser must support SSL (i.e. https).)

- ☐ Make certain that the browser does not automatically setup a connection when it starts, because otherwise the connection startup to the RR-EPL could be impaired.
In MS Internet Explorer, you can prevent this with the following setting:
In the `Extras` menu, select `Internet Options...` and click on the `Connections` tab. Make certain that "Never dial a connection" is selected under `Dial-up and Virtual Private Network` settings.
- ☐ Enter the complete address of the RR-EPL into the browser's address field.

Afterwards:

The RR-EPL's Administrator Web page will be displayed. The security notice shown on the next page will displayed.

Note: If the Administrator Web page is not displayed...

If - even after repeated attempts - the browser still reports that the page cannot be displayed, try the following:

- ▶ Check if both ports have a network connection.
- ▶ Try disabling any existing firewall.
- ▶ Make certain that the browser does not use a proxy server.
In MS Internet Explorer (Version 6.0), you can prevent this with the following setting: In the `Extras` menu, select `Internet Options...` and click on the `Connections` tab. Under `LAN Settings` click on the `Properties...` button and, in the `Local Area Network (LAN) Settings` dialog, check to make certain that `Use a proxy server for your LAN (under Proxy server)` is not activated.
- ▶ If any other LAN connection is active on the system, deactivate it until the configuration has been completed.
Under the `Windows Start menu:Settings:Control Panel:Network Connections` or `Network and Dial-up Connections`, right click on the associated icon and select `Disable` in the pop-up menu.

5.1.2 After a successful connection setup

After the connection has been successfully setup, the following security notice will be displayed (MS Internet Explorer):

Since administrative tasks can only be performed when a secure (encrypted) access has been established to the device, a signed (by the device) certificate will be returned.

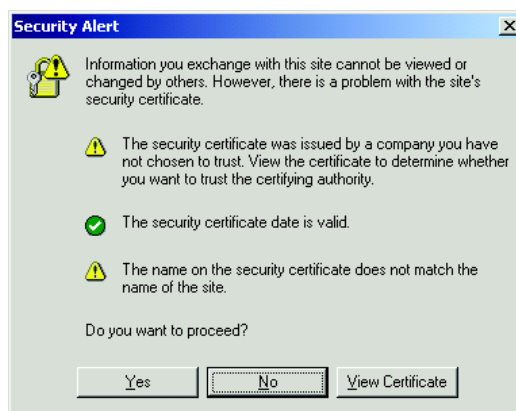


Fig. 17: Security notice dialog

- ☐ Acknowledge the associated security notice by clicking on **Yes**.

Afterwards:

Once you have entered the correct user name (Login) and password, the Administrator Web page of the RR-EPL will be displayed.

Name	Entry
Login	admin
Password	private

Table 3: Factory settings for login name and password

Note: These entries are case-sensitive!

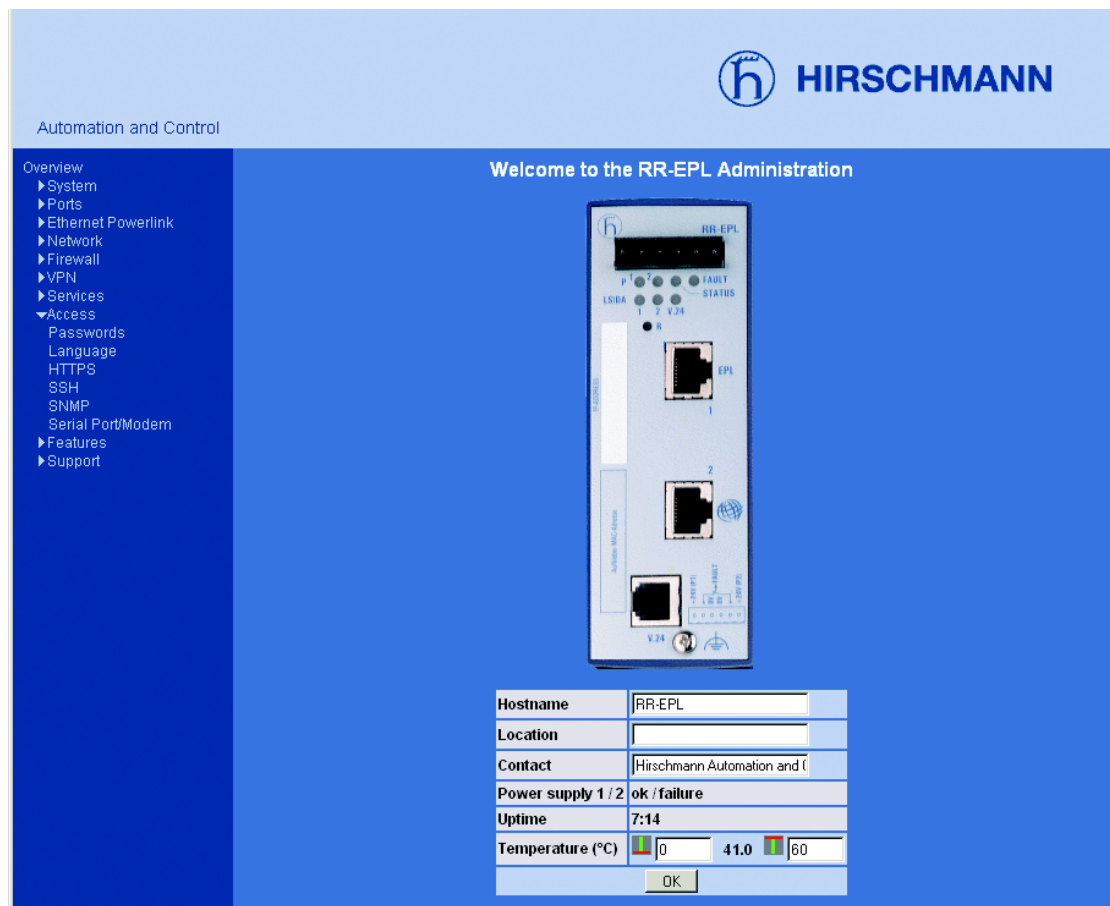


Fig. 18: Administrator website start screen

To configure the device, proceed as follows:

- ☐ Call up the desired dialog - see [“Web-based management” on page 53](#).
- ☐ Make the desired settings on the associated page
- ☐ Once you have confirmed the changes by clicking on **OK**, the new settings will be activated on the device.
You may receive a message from the system (confirmation).

If the changes are not shown when you open the page again, because the browser has loaded the page from a cache, reload the page to refresh the display. To do so, click on the appropriate icon in the browser toolbar.

Note: Depending on how you configure the RR-EPL, you may also need to modify the network interface settings of the locally connected system or network accordingly.

5.2 Remote configuration

Prerequisites:

The RR-EPL must be configured via the unsecure port. For reasons of security, remote configuration is disabled by default.

For information on how to enable remote configuration, see [“Access:HTTPS” on page 139](#).

5.2.1 Remote configuration via LAN

To configure the RR-EPL from a remote computer, first establish a connection between it and the local RR-EPL.

Proceed as follows:

- ☐ Start a Web browser (e.g. MS Internet Explorer Version 5.0 or later or Netscape Communicator Version 4.0 or later; the Web browser must support SSL (i.e. https) on the remote system).
- ☐ As the URL, enter: the IP address under which the remote site can be reached via the Internet or WAN, plus the port number.

Example:

If this RR-EPL can be found in the Internet at the address 192.144.112.5 and the Port Number 443 has been set as the port for remote access, you must enter the following address in the Web browser's address field on the remote system: 192.144.112.5

(If a different Port Number is used, this must be appended to the IP address, e.g.: 192.144.112.5:442)

Hinweis: For reasons of security, we recommend that you change the default Root and Administrator passwords during the first configuration - see [“Access:passwords” on page 136](#).

5.2.2 Remote configuration via modem

The V.24 port allows you to,

- ▶ perform remote maintenance in transparent mode RR-EPL
- ▶ perform remote maintenance on the RR-EPL in router mode and on the secure network behind it

via a modem (e.g. INSYS modem 56K small).

Access to the secure network is subject to the firewall rules in this dialog.

■ Local installation:

- ☐ Connect your modem on the one end to the telephone network and on the other end to the V.24 port of the RR-EPL via the mode cable (see [“Accessories” on page 193](#)).

■ Remote installation:

- ☐ Connect your PC to the telephone network via the built-in or external modem.

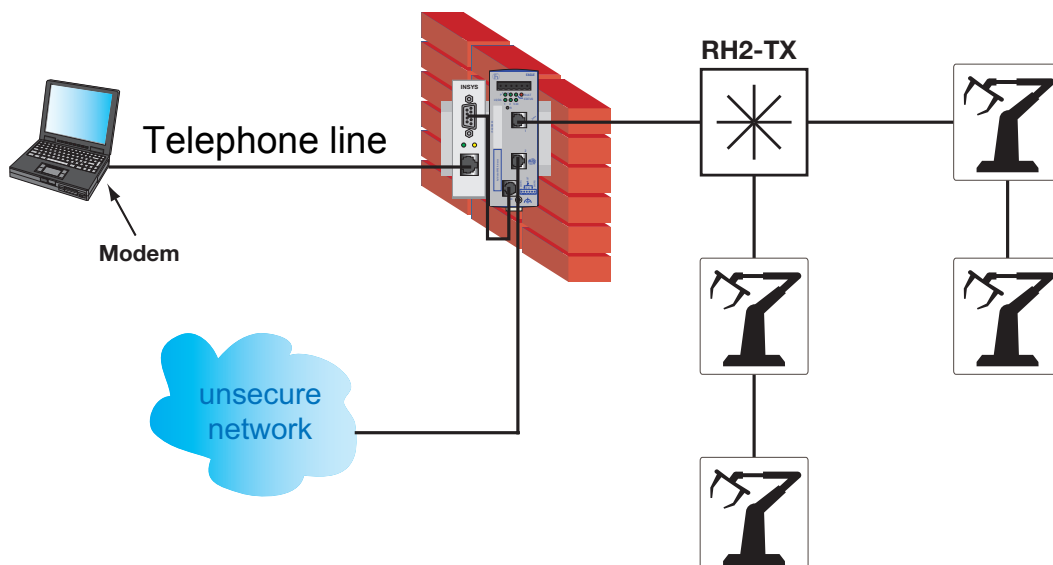


Fig. 19: Example of a modem connection

Example of establishing a modem connection under Windows 2000:

☐ **Choose:**

Start:Settings:Network and Dial-Up Connections:Make New Connection
and continue with the Network Connection Wizard (see the following two figures). Enter the phone number at which you can reach the modem.

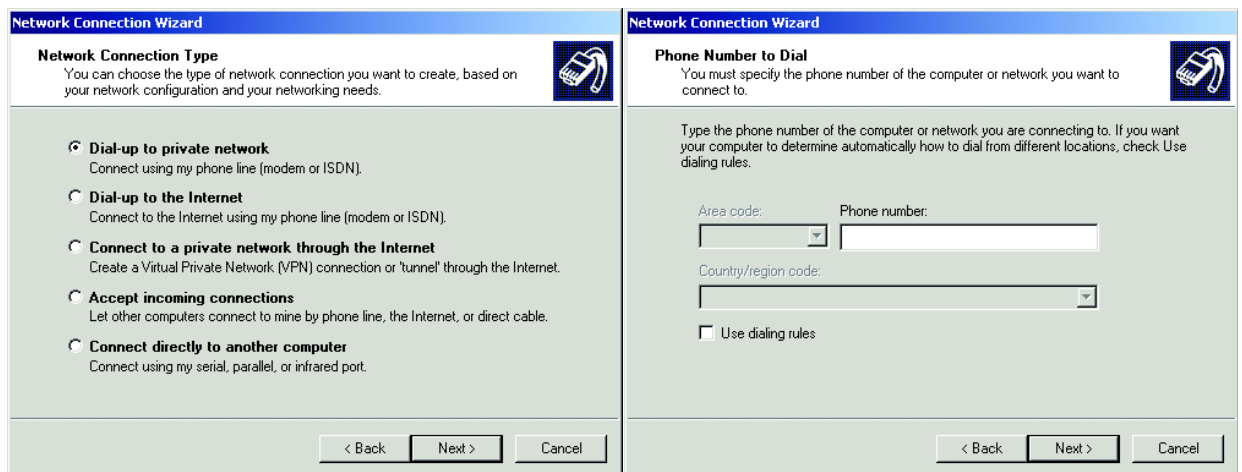


Fig. 20: Network connection type, phone number



Select "Properties" to check the settings for the connection (see the following two figures).

Fig. 21: Establishing a connection

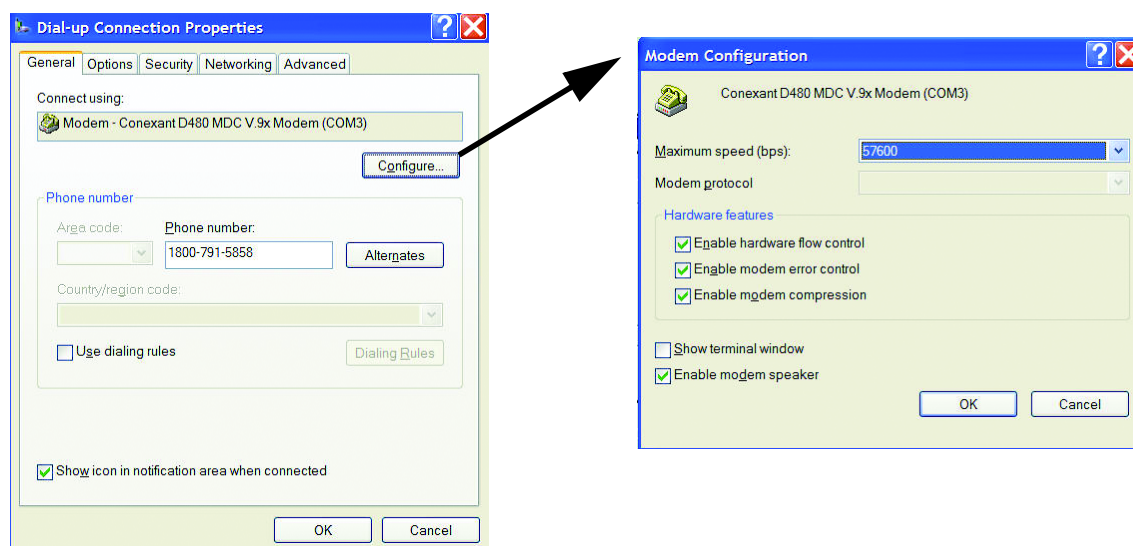


Fig. 22: General connection properties

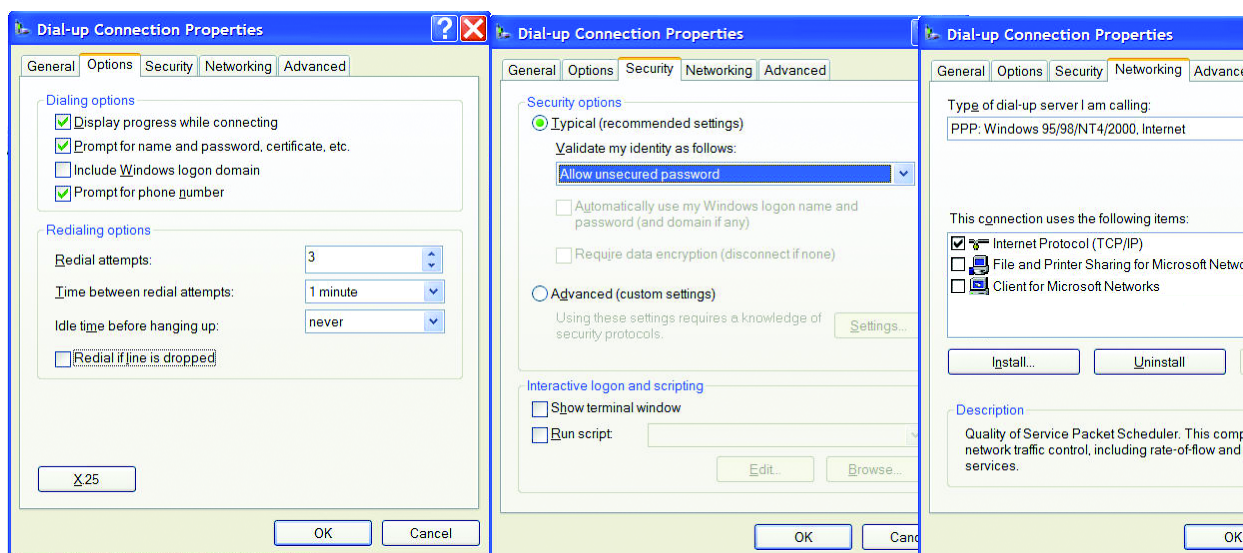


Fig. 23: Connection properties: Options, security and network

After a connection has been set up, the connection symbol will appear in the task bar tray at the bottom right.

☐ Left-click the connection symbol and select *Status*.

☐ In the status window click the register card "Details".

This register card contains the

IP address of the RR-EPL (= server IP address).

☐ Enter `https://` followed by this IP address in the address bar of your browser to establish the connection to the RR-EPL's Web-based administrator user interface.

Requirement: Configuration of the serial interface (see the following figure).

Access > Serial Port/Modem

Serial connection, modem, PPP

Baudrate: 9600

MODEM(PPP): Off

Hardware handshake RTS/CTS: Off

PPP dialin options

Local IP: 192.168.2.1

Remote IP: 192.168.2.2

PPP Login name: admin

PPP Password: [password]

Firewall Incoming (PPP interface)

Protocol	From IP	From Port	To IP	To Port	Action	Comment	Log
Log entries for unknown connection attempts							
							No

Firewall Outgoing (trusted port)

Protocol	From IP	From Port	To IP	To Port	Action	Comment	Log
Log entries for unknown connection attempts							
							No

OK

In addition to the rules you configured above the PC dialed in via PPP has IP access to HTTPS, SSH and SNMP management. With the rules above you can configure additional access to the internal or external network.

Please note: It's not possible to connect a serial modem to the mGuard smart.

Fig. 24: Configuring the serial interface

6 Web-based management

The RR-EPL supports both SNMP management and Web-based management and can thus offer

- ▶ extensive diagnostic and configuration functions for fast startup and
- ▶ extensive network and device information.

The RR-EPL supports the TCP/IP protocol family.

The user-friendly Web-based interface gives you the option of managing the MICE from any location in the network via a standard browser such as the Netscape Navigator/Communicator or the Microsoft Internet Explorer. The Web-based interface allows you to graphically configure the RR-EPL.

■ Editing tables

A number of dialogs contain tables. The tables are all used in the same way.

Creating a new table entry:

- ☐ Click on a “downward arrow” symbol on the left side of the table.
You thus create an entry below the symbol you clicked on.

Moving an existing table entry:

- ☐ Select a row on the left side of the table below the “X” symbol.
- ☐ By clicking on a “downward arrow” symbol you move the row to below the clicked symbol.

Deleting an existing table entry:

- ☐ Select the row to be deleted on the left side of the table below the “X” symbol.
- ☐ You click on the “X” symbol to delete the selected row.

Editing the comment column:

You can use the fields in the comment column to add remarks for every table entry.

6.1 Overview

The Overview dialog shows you a graphic display of the RR-EPL and the system data:

- ▶ Name: any name you wish to assign to the RR-EPL for easier identification.
- ▶ Location: Location of this RR-EPL.
- ▶ Power supply 1/2: Status of the power supply units.
- ▶ Uptime: Time that has elapsed since the RR-EPL was last restarted.
- ▶ Temperature, displays the temperature inside the RR-EPL. Enter the lower and upper temperatures as alarm thresholds.

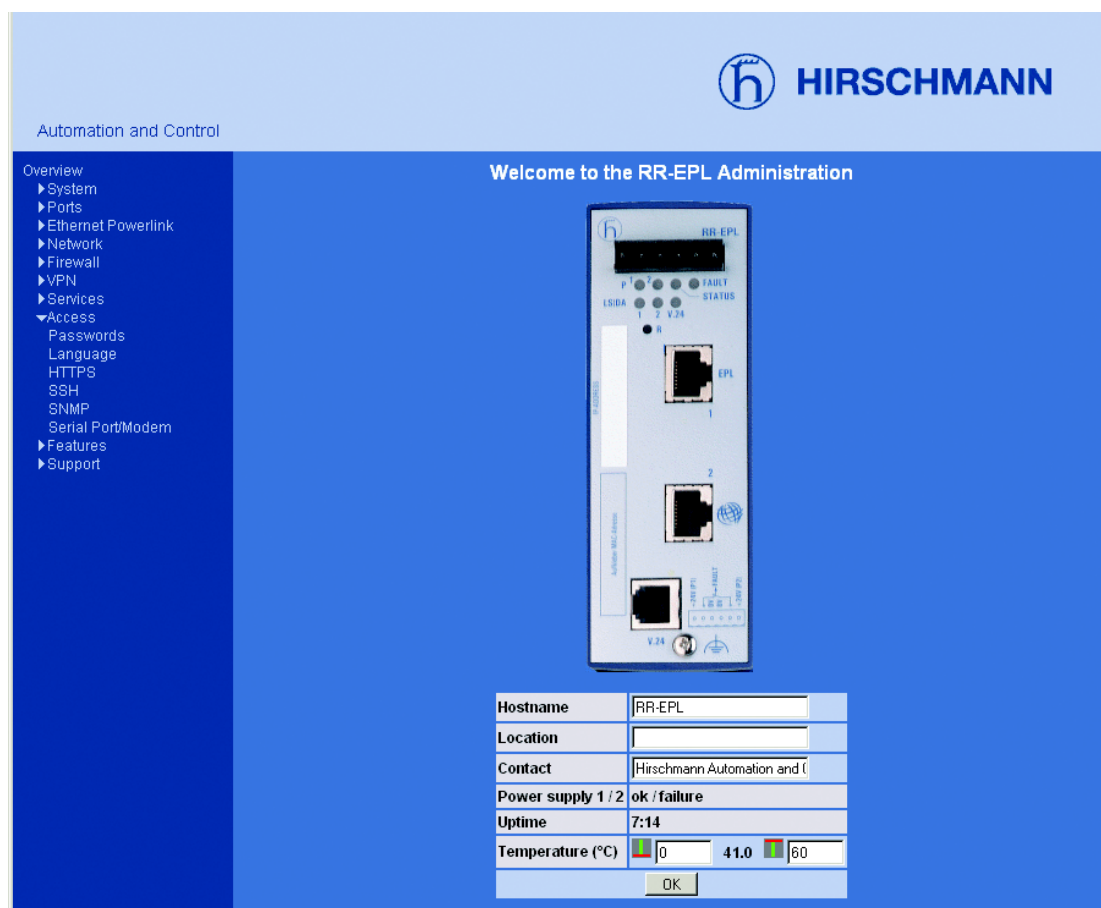


Fig. 25: System data

6.2 System menu

6.2.1 System:Configurations-Profiles

You can save the configuration settings as a configuration profile under any name in the RR-EPL. You can create and save multiple configuration profiles. You can then select and activate the configuration profile appropriate at the time, if you use the RR-EPL in different operating environments.

Furthermore, you can also save configuration profiles as files on the configuration system. Naturally, these configuration files can then be read back into the RR-EPL and activated.

Furthermore, you can restore the RR-EPL to the factory settings at any time.

Note: Passwords and user names are not saved in the configuration profiles.

Note: With `Save Current Configuration to ACA 11` you save the current configuration on the ACA 11, if it is connected. Enter the valid `root` password.

System > Configuration-Profiles

Name
Factory Default

Restore Download

Name for the new profile: Save Current Configuration to Profile

Durchsuchen... Upload Configuration to Profile

The root password to save on ACA11: Save Current Configuration to ACA11

Fig. 26: Configuration profiles

■ Saving the current configuration in the RR-EPL as a profile

- ☐ In the Name for the new profile: field, enter the desired name.
- ☐ Click on the Save Current Configuration to Profile button.

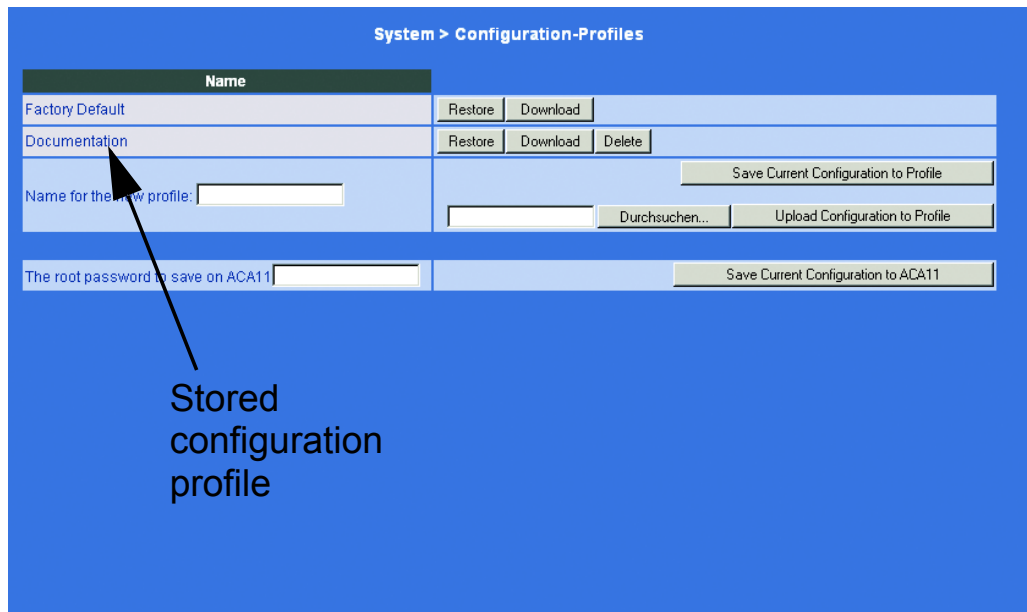


Fig. 27: Example of a stored configuration profile

■ Display / Activate / Delete a configuration profile stored in the RR-EPL

Requirement: At least one configuration profile has been created and is stored in the RR-EPL (see above).

- Display the configuration profile:
Click the name of the configuration profile.
- Activate the configuration profile:
Click the `Restore` button next to the right of the respective configuration profile.
- Delete the configuration profile:
Click the `Delete` button to the right of the respective configuration profile.

■ **Factory default settings - displaying / activating**

The default setting is stored in the RR-EPLas configuration profile under the name `Factory Default`.

- ▶ **Displays:** Click the name `Factory Default`.
- ▶ **Activate:** Click the `Restore` button next to the name `Factory Default`.
It is not possible to delete the configuration profile `Factory Default`.

■ **Saving a configuration profile as a file on a hard disk**

- ☐ Click on the `Download` button at the right of the name of the configuration profile.
- ☐ Enter the filename and folder (where the configuration profile should be saved) in the displayed dialog. You can give the file any name desired.

■ **Uploading a configuration profile from a hard disk to the RR-EPL**

Prerequisite: Naturally, you must stored (as described above) at least one configuration profile as a file on the hard disk of the configuration system.

- ☐ In the `Name for the new profile` field, enter the name that should be assigned to configuration profile uploaded from the disk.
- ☐ Click on `Choose` and then select the file.
- ☐ Click on the `Upload Configuration to Profile` button.
Afterwards: The uploaded configuration will now be displayed in the list of configuration profiles.
- ☐ If you want to activate the uploaded configuration profile, click on the `Restore` button next to the name.

Note: If the restore procedure involves changing from the transparent mode to another network mode, the RR-EPL will be restarted. If the ACA 11 is connected, the RR-EPL will obtain the configuration data from the ACA 11.

6.2.2 System:Configuration Pull

This dialog allows you to specify when the RR-EPL automatically downloads a configuration from a server and continues working with this configuration.

Parameter	Meaning
Pull schedule	Period after which the RR-EPL downloads a configuration from a server. Possible: <ul style="list-style-type: none">- Never (state on delivery)- Once at boot- Every 15 min- Every 30 min- Every 1 h- Every 2 h- Every 6 h- Every 12 h- Every 24 h
Server	Path and file name of the configuration file to be loaded.
Login	Login name for the server.
Password	Password for the login name.
Server certificate	Certificate for checking the validity of the configuration file.

Table 4: Settings for automatically pulling a configuration

6.2.3 System:Reboot

At the end of restart, the text appears “Restarted.”

A reboot can be initiated by switching the device off and then back again or by pressing the Recovery button (see [“Performing a restart” on page 166](#)).

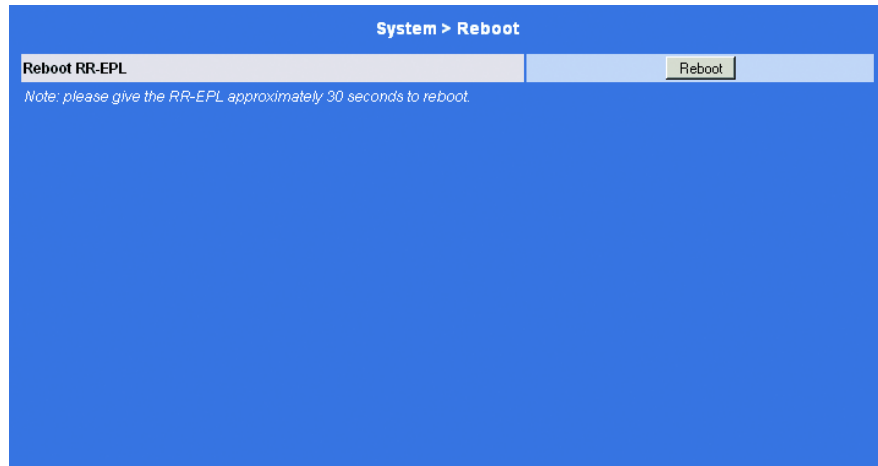


Fig. 28: Reboot

6.2.4 System:Logs - Display

Displays all recorded log entries (overall system log). For a selection of specific log entries, see the respective dialogs (see for example [“VPN:VPN Logs - Display”](#) on page 116).

The format of the log corresponds to that common under Linux

Special analysis programs are available which can be used to present the information from the log in a more readable format.

You can send the logged entries to an external server (see [“Services:Remote Logging”](#) on page 131).

```

uptime 0 days 00:00:06.60216 main: listening on /dev/log, starting.
uptime 0 days 00:00:07.40432 sshd[168]: Server listening on 0.0.0.0 port 22.
uptime 0 days 00:00:07.77927 kernel: mGuard: kernel sniffer registered.
uptime 0 days 00:00:07.77940 kernel: mGuard: sysctl directory registered.
uptime 0 days 00:00:07.77950 kernel: mGuard: procfs entries created.
uptime 0 days 00:00:07.77961 kernel: Interfaces: int:'eth1', ext:'eth0'
uptime 0 days 00:00:07.81140 root: Using /lib/modules/2.4.25-mg-4.6.44/kernel/net/mguard/mguard.o
uptime 0 days 00:00:07.81158 root: Warning: loading mguard will taint the kernel: non-GPL license - Pr
uptime 0 days 00:00:07.81170 root: See http://www.tux.org/lkml/#export-tainted for information about
uptime 0 days 00:00:07.90397 kernel: ip_conntrack version 2.1 (512 buckets, 4096 max) - 328 bytes per
uptime 0 days 00:00:07.90501 root: Using /lib/modules/2.4.25-mg-4.6.44/kernel/net/ipv4/netfilter/ip_co
uptime 0 days 00:00:07.93869 kernel: ctnetlink v0.12: registering with nfnetlink.
uptime 0 days 00:00:07.93963 root: Using /lib/modules/2.4.25-mg-4.6.44/kernel/net/ipv4/netfilter/nfnet
uptime 0 days 00:00:07.96566 root: Using /lib/modules/2.4.25-mg-4.6.44/kernel/net/ipv4/netfilter/ipt_s
uptime 0 days 00:00:08.03672 root: Using /lib/modules/2.4.25-mg-4.6.44/kernel/net/ipv4/netfilter/iptak
uptime 0 days 00:00:08.05602 root: Using /lib/modules/2.4.25-mg-4.6.44/kernel/net/ipv4/netfilter/ipt_I
uptime 0 days 00:00:08.08386 root: Using /lib/modules/2.4.25-mg-4.6.44/kernel/net/ipv4/netfilter/ipt_L
uptime 0 days 00:00:08.11072 root: Using /lib/modules/2.4.25-mg-4.6.44/kernel/net/ipv4/netfilter/iptak
uptime 0 days 00:00:08.13819 root: Using /lib/modules/2.4.25-mg-4.6.44/kernel/net/ipv4/netfilter/ipt_L
uptime 0 days 00:00:08.15680 root: Set name-type for VLAN subsystem. Should be visible in /proc/net/v
uptime 0 days 00:00:16.23852 getty: GETTY detected hardware 3 (1=smart 2=pci 3=industrial) 00000207,
uptime 0 days 00:00:16.23978 getty[1192]: starting, modem=0, baudrate=9600, modem_reset:ATEO
uptime 0 days 00:00:17.61455 root: psm-boot: info: done.
uptime 0 days 00:00:24.06042 kernel: ixp425_eth: eth0: Entering promiscuous mode
uptime 0 days 00:00:24.06055 kernel: device eth0 entered promiscuous mode
uptime 0 days 00:00:24.07010 kernel: ixp425_eth: eth1: Entering promiscuous mode
uptime 0 days 00:00:24.07024 kernel: device eth1 entered promiscuous mode
uptime 0 days 00:00:24.11067 kernel: br0: port 2(eth1) entering learning state
uptime 0 days 00:00:24.11082 kernel: br0: port 1(eth0) entering learning state

```

Fig. 29: Logs

6.2.5 System:HiDiscovery

The HiDiscovery protocol allows you to assign the RR-EPL an IP address based on its MAC address. Activate the HiDiscovery protocol if you want to assign an IP address to the RR-EPL from your PC with the enclosed HiDiscovery software (setting on delivery: active).

Note: For security reasons, the RR-EPL HiDiscovery function supports only the secure port

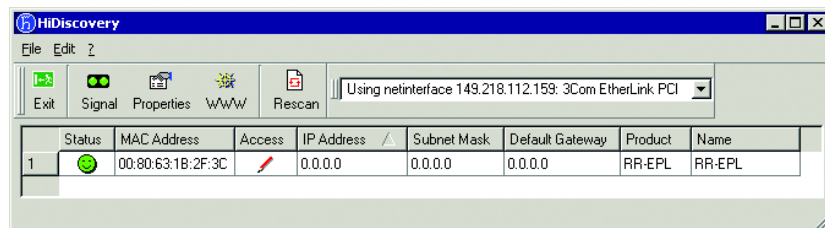


Fig. 30: HiDiscovery

■ Local HiDiscovery Support

(unsecure port only)

- ▶ Enabled, local IP address assignment via HiDiscovery possible.
- ▶ Read-Only, HiDiscovery can read local parameters.
- ▶ Disabled, no HiDiscovery access to local parameters possible.

6.2.6 System:Signal contact

The signal contact is for

- ▶ manual setting the signal contact.
- ▶ monitoring proper functioning of the RR-EPL and enables remote diagnostics.

■ Signal contact

Setting the function of the signal contact:

- ▶ Operational supervision
- ▶ Manual setting

■ Operational supervision

A break in contact is reported via the zero-potential signal contact (relay contact, closed circuit):

- ▶ the failure of at least one of the two supply voltages (power supply voltage 1 or 2 < 9,6 V).

Note: With a non-redundant supply of the supply voltage, the RR-EPL will report a supply power failure. You can prevent this by

- feeding the supply voltage over both inputs or
 - by selecting “Ignore redundant power supply”.
- ▶ the defective link status of at least one port. The link status message can be masked for
 - Ignore: no link monitor
 - Supervise only internal port (trusted): EPL port
 - Supervise only external port (untrusted)
 - Supervise both ports
- Link status is not monitored in the delivery condition.

■ Manual settings

This mode gives you the option of remote switching the signal contact.

☐ Select `Open (Alarm)` to open the contact.

☐ Select `Closed` to close the contact.

Application options:

► Simulation of an error during SPS error monitoring.

► Remote control of a device via SNMP, such as switching on a camera.

System > Signal contact

Mode

Signal contact Operation supervision ▼

Operation supervision

Contact [Open (Error)]

Redundant power supply Supervise ▼

Link supervision Ignore ▼

Manual settings

Contact Closed ▼

OK

Fig. 31: Signal contact

6.3 Ports menu

6.3.1 Ports:Configuration Table

This table allows you to configure every port of the RR-EPL.

Ports > Configuration Table						
Port	Media Type	Link State	Automatic Configuration	Manual Configuration	Current Mode	Port On
Internal/Trusted	10/100 BASE-T/RJ45	Up	<div>Yes</div>	<div>100 Mbit/s FDX</div>	100 Mbit/s FDX	<div>Yes</div>
External/Untrusted	10/100 BASE-T/RJ45	Up	<div>Yes</div>	<div>100 Mbit/s FDX</div>	100 Mbit/s FDX	<div>Yes</div>
<div>OK</div>						

Fig. 32: Port configuration

Automatic Configuration

In the “Automatic Configuration” (Autonegotiation) column, you can activate the automatic selection of a port's operating mode by marking the appropriate field. After the au-tonegotiation has been switched on, it takes a few seconds for the oper-ating mode to be set.

Manual Configuration

In the “Manual Configuration” column, you set the operating mode for this port. The choice of operating modes depends on the media module. The possible operating modes are:

- ▶ 10 Mbit/s half duplex (HDX),
- ▶ 10 Mbit/s full duplex (FDX),
- ▶ 100 Mbit/s HDX and
- ▶ 100 Mbit/s FDX.

Note: The active automatic configuration has priority over the manual configuration.

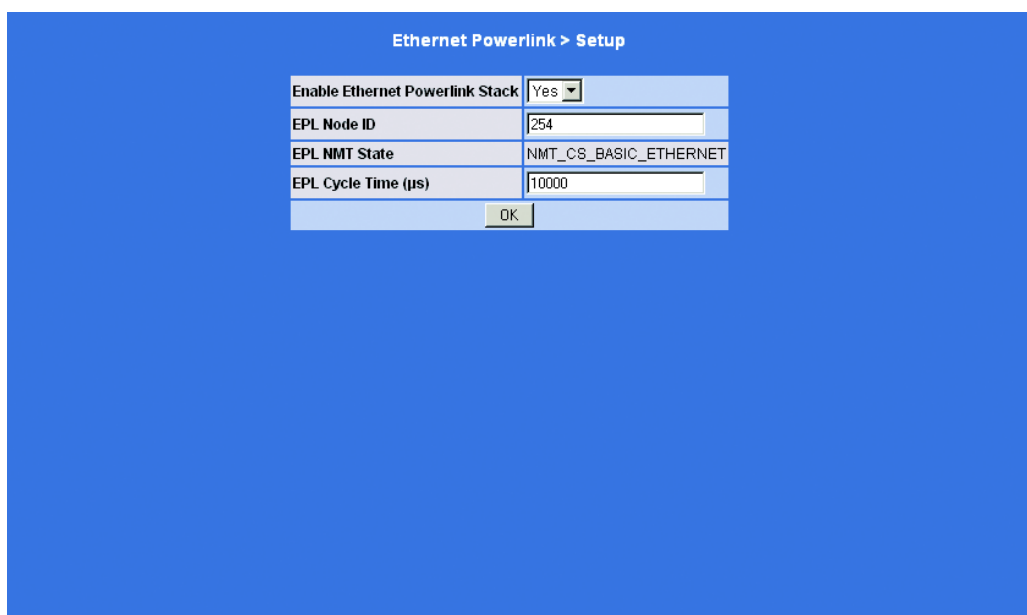
■ **Switching a port on and off**

With the “Port on” column, you can switch a port on and off.

6.4 Ethernet Powerlink menu

6.4.1 Ethernet Powerlink: Setup

This dialog allows you to configure the RR-EPL as an Ethernet Powerlink node.



Ethernet Powerlink > Setup	
Enable Ethernet Powerlink Stack	Yes
EPL Node ID	254
EPL NMT State	NMT_CS_BASIC_ETHERNET
EPL Cycle Time (µs)	10000
OK	

Fig. 33: Ethernet Powerlink Setup

■ Enable Ethernet Powerlink Stack

With „Enable Ethernet Powerlink Stack“ you enable/disable the function.
Default setting: Yes.

■ EPL Node ID

Here you enter the EPL node ID under which the managing node will address the RR-EPL.
Specification Object: 0x1F93 Sub-Index: 2.
Default setting: 254.

■ EPL NMT State

In this line the RR-EPL displays the status of the NMT state machine.

Possible values:

- ▶ NMT_CS_PRE_OPERATIONAL_1
- ▶ NMT_CS_PRE_OPERATIONAL_2
- ▶ NMT_CS_READY_TO_OPERATE
- ▶ NMT_CS_OPERATIONAL
- ▶ NMT_CS_STOPPED
- ▶ NMT_CS_BASIC_ETHERNET

■ EPL Cycle Time (µs)

Here you enter the EPL cycle time in microseconds.

Specification: Object 0x1006.

Default setting: 10000.

Note: When you select “OK”, the RR-EPL saves these settings in the configuration. To transfer the settings to the EPL stack, you use `Ethernet Powerlink:Reset` to reset the EPL stack or execute the NMT command `ResetConfiguration`.

6.4.2 Ethernet Powerlink:Reset

This dialog allows you to reset the EPL stack and restart it with the saved configuration.

This may be necessary in order to reset the status

NMT_CS_PRE_OPERATIONAL_1, which is taken from the RR-EPL in the case of managing node failure, in accordance with the EPL specification, back to the NMT_CS_BASIC_ETHERNET mode.

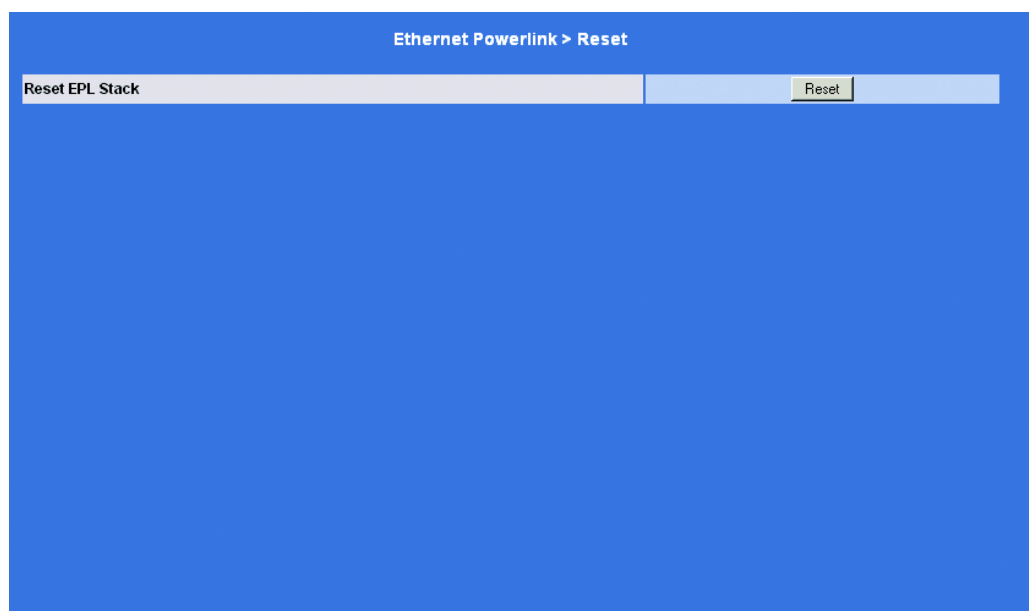


Fig. 34: Ethernet Powerlink Reset

6.4.3 Ethernet Powerlink:SDO Access

With this dialog you can enter settings for the SDO access. SDO (Service Data Object) provides the access to all the variables in a CANopen device.

■ **Enable SDO remote access**

If you wish to enable SDO remote access, set this switch to `Yes`.

Note: Ensure that in this case the firewall rules on this end have been set so that it is possible to access the RR-EPL from an external terminal.

■ **Port for SDO connections (remote administration only)**

Standard: 3819

You can set another port.

The remote terminal that performs the remote access must add the port number defined here to the end of the IP address when it assigns the address.

Example:

If this RR-EPL can be reached at the address 192.144.112.5 over the Internet, and if port number 3819 has been set for remote access, this port number does not have to be specified in the SDO client.

■ **Firewall rules to accept external SDO access**

Lists the firewall rules that have been established. They apply to the incoming data packets of an SDO remote access connection.

► Editing rule

Define the desired rule (see above) and click `OK`.

► From IP

Enter the address(s) of the computer(s) which is/are permitted remote access.

The following entry options are available:

– IP address: `0.0.0.0/0` means all addresses. To indicate a range, use the CIDR notation - see [“CIDR \(Classless InterDomain Routing\)” on page 160](#).

► Interface

external (fixed)

- **Action**
Options: Accept / Reject / Drop

Action	Meaning
Accept	the data packets are permitted to pass through.
Reject	the data packets are rejected, and the sender is notified that the data was rejected. In transparent mode, <code>Reject</code> has the same effect as <code>Discard</code> , see above.
Drop	the data packets are not permitted to pass through. They are “swallowed”, and the sender is not notified about what happened to the data.

Table 5: Actions for HTTPS access

- **Log**
For each individual firewall rule you can decide if, when the rule is applied,
- the event should be logged – set Log to `Yes`
 - or not – set Log to `No` (factory default setting).

Ethernet Powerlink > SDO Access

Enable SDO remote access Yes

Port for incoming SDO connections (external interface only) 3819

Firewall rules to accept SDO access:

	From IP	Interface	Action	Comment	Log
<input type="checkbox"/>	0.0.0.0/0	External	Accept		No

OK

These rules allow to enable SDO remote access.
 Note: Both global SDO remote access must be enabled and firewall rules allowing access from a chosen IP address range must set.
 Note: In Transparent mode incoming traffic on the given port is no longer forwarded to the client.
 Note: In router mode with NAT or portforwarding the port set here has priority over portforwarding.
 Note: The SDO access from the internal side is enabled by default and can be restricted by firewall rules.

Fig. 35: Ethernet Powerlink SDO Access

6.4.4 Protecting the EPL segment

In the basic setting, every station in the legacy Ethernet can access the EPL cell. You can restrict this access by means of corresponding firewall rules. Entries can be made in the following menus to restrict the access to the EPL cell:

- ▶ Firewall > Incoming (untrusted port)
Here you can include or exclude stations or parts of the network from accessing the EPL segment.

It can also be useful for you to restrict the access to the RR-EPL itself, using the following menus:

- ▶ Access > HTTPS
- ▶ Access > SSH
- ▶ Access > SNMP
- ▶ Ethernet Powerlink > SDO Access

6.4.5 Ethernet Powerlink:Logs - Display

Displays the LOG entries specific to the Ethernet Powerlink which the RR-EPL makes for various EPL events.

6.5 Network menu

6.5.1 Network:Base

The RR-EPL must naturally be set to the Network Mode (= operating mode) that matches its connection to the local computer or network (see “[Typical application scenarios](#)” on page 19).

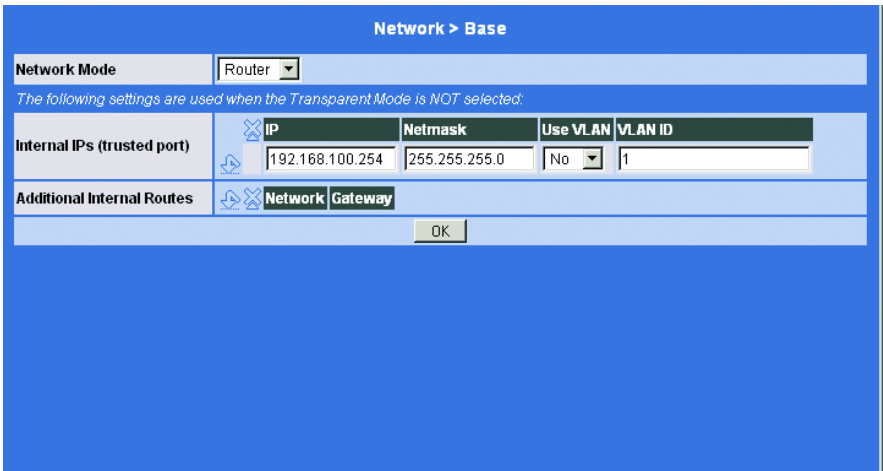


Fig. 36: Network:Base

Variable	IP address
in router mode (at EPL port)	192.168.100.254
in PPPoE mode	192.168.100.254
Local netmask	255.255.255.0

Table 6: The RR-EPLs preset local IP address

Note: When the Network Mode has been changed, the device will reboot automatically.

Note: If you change the address of the RR-EPL (e.g. by changing the Network Mode from Router to PPPoF), the device will be immediately, after a restart, only accessible at the new address.

Note: If you set the Network Mode to Router, PPPoE or PPTP and then change the internal IP address and/or the local netmask, make very certain that you enter the correct values. Otherwise, the RR-EPL will no longer be accessible.

■ Network mode

► Router mode

This is the normal mode of the RR-EPL.

The security functions firewall and VPN are available.

Note: If the RR-EPL is operated in router mode, a locally connected client computer of the RR-EPL must be defined as the standard gateway, i.e. the address of the standard gateway must be set to the internal IP address of the RR-EPL (see [“IP configuration for the Windows clients” on page 127.](#))

Note: If the RR-EPL is operated in Router mode and is used to establish the connection to the Internet, you should activate NAT to allow access to the Internet from the local network (see [“Firewall:NAT” on page 90](#)). If NAT is not activated, the device will only allow VPN connections.

► PPPoE mode

The PPPoE mode corresponds to router mode with DHCP – with one difference: To connect to an external network (Internet, WAN) the PPPoE protocol is used – as in Germany – which is used by many DSL modems (for DSL Internet access). The external IP address, at which the RR-EPL can be reached from a remote terminal, is determined dynamically by the provider.

Address of the device (for configuration purposes):

IP address: 192.168.1.1

Local network mask: 255.255.255.0

Note: If the RR-EPL is operated in PPPoE mode, a locally connected client computer of the RR-EPL must be defined as the standard gateway, i.e. the address of the standard gateway must be set to the internal IP address of the RR-EPL (see [“IP configuration for the Windows clients” on page 127.](#))

Note: If the RR-EPL is in PPPoE mode, NAT must be activated to enable access to the Internet (see [“Firewall:NAT” on page 90](#)). If NAT is not activated, the device will only allow VPN connections.

► **PPTP Mode**

This mode is similar to PPPoE mode. In Austria, for example, PPTP is used instead of the PPPoE protocol for DSL connections. PPTP is the protocol, which was originally used by Microsoft for VPN connections.

Note: If the RR-EPL is operated in PPTP mode, you must set it as the standard gateway in the locally connected client computers. In other words, the address entered for the standard gateway must be the internal IP address of the RR-EPL (see [“IP configuration for the Windows clients” on page 127](#)).

Note: If the RR-EPL is in PPTP mode, NAT must be activated to enable access to the Internet (see [“Firewall:NAT” on page 90](#)). If NAT is not activated, the device will only allow VPN connections.

■ **Internal IPs**

Router / PPPoE / PPTP mode

`Internal IPs` is the IP address, under which the RR-EPL can be accessed from the locally connected LAN.

Default setting:

IP address: 192.168.100.254

Lokal Netmask: 255.255.255.0

VLAN: no

VLAN ID: 1

You can also specify other addresses, under which the RR-EPL can be accessed by devices on the locally connected network. This can be useful, for example, if the locally connected network is divided into subnetworks. In this case, multiple units on different subnetworks can access the RR-EPL under different addresses (multinetting).

- ☐ If you wish to define another internal IP, click the arrow down.
- ☐ If you wish to delete an internal IP, select the line and click the „X“ symbol.

The first IP address in the list cannot be deleted.

■ Additional Internal Routes

Router / PPPoE / PPTP mode

If the locally connected network includes subnetworks, you can define additional routes.

Also see [“Example of a network” on page 162](#).

- ☐ If you wish to define another route to a subnetwork, click on **New**.

Enter:

- the IP address of the subnetwork (network), plus
- the IP address of the gateway through which the subnetwork is connected.

You can define any number of internal routes.

- ☐ If you wish to delete an internal route, click the „X“ symbol.

Note: If additional internal routers are defined, these have no effect in transparent mode.

6.5.2 Network:Router

Requirement: The RR-EPL has been set to the network mode Router.

Network > Router

External Interface

Obtain external configuration via DHCP No

If 'DHCP' is set to 'No', the following values need to be configured:

External Networks

	IP	Netmask	Use VLAN	VLAN ID
External IPs (untrusted port)	10.0.0.152	255.255.255.0	No	1

Additional External Routes

Network Gateway

Default Gateway

IP of default gateway

10.0.0.253

OK

Fig. 37: Network:Router

■ External interface

Obtain external configuration via DHCP: Yes / No.

- ☐ If the RR-EPL obtains the configuration data per DHCP (Dynamic Host Configuration Protocol) from the DHCP server, set Yes. No other information is necessary.
- ☐ If the RR-EPL does not obtain the data via DHCP (Dynamic Host Configuration Protocol) from the DHCP server, set No.

The RR-EPL must then operate in the network mode Router (see “Router mode” on page 73). You must then make provide further information:

■ External networks (connected to the insecure port)

External IPs (untrusted port)

At these external IP addresses, the RR-EPL can be reached by devices of the external network (connected to the Ethernet socket of the RR-EPL). They form the interface to other parts of the LAN or to the Internet. If the gateway to the Internet is here, the IP address are then determined by the Internet service provider (ISP).

- ☐ If you wish to provide an additional external IP, click “New”.
- ☐ If you wish to delete one of the external IPs, click the “X” symbol.

Additional External Routes

In addition to the default route (see below) you can define other external routes.

- ☐ If you wish to provide an additional external route, click the arrow down.
- ☐ If you wish to delete one of the additional external routes, click the “X” symbol.

See also [“Example of a network” on page 162](#).

■ Default Gateway

Default of default gateway

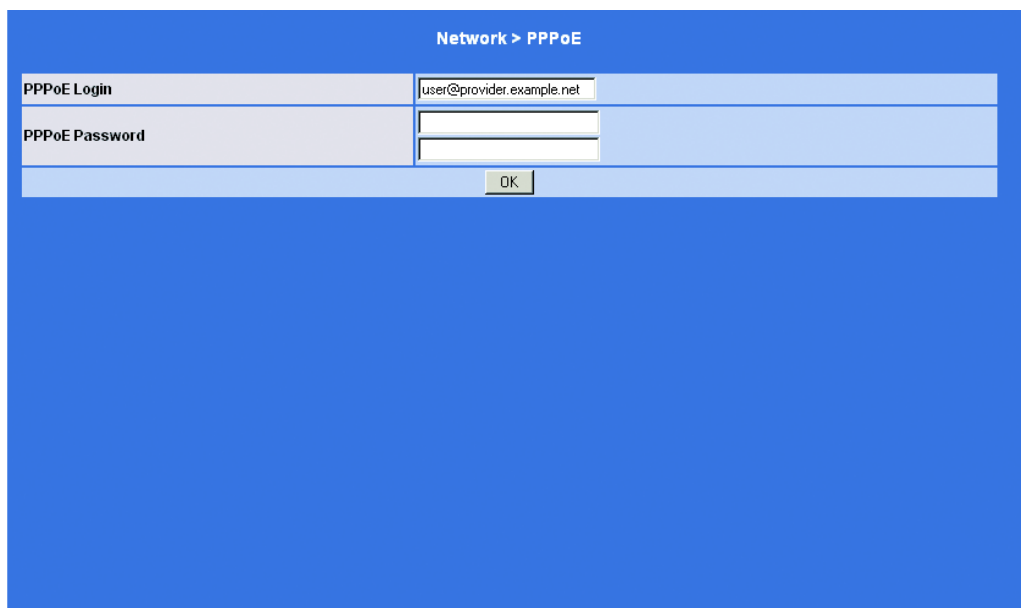
Is determined by the Internet service provider (ISP), when the RR-EPL sets up the gateway to the Internet. If the RR-EPL is used within the LAN, the route from the network administrator is specified.

Note: If the local network is not known to the external router, e.g. in the case of configuration by DHCP, enter the address of your local network under `Firewall:NAT`, in other words `0.0.0.0/0` (see [“Firewall:NAT” on page 90](#)).

6.5.3 Network:PPPoE

Requirement: The RR-EPL has been set to the network mode PPPoE.
(see [“PPPoE mode” on page 73](#)).

User name (login) and password are requested by the Internet Service Provider (ISP), when you wish to establish a connection with the Internet.



Network > PPPoE	
PPPoE Login	<input type="text" value="user@provider.example.net"/>
PPPoE Password	<input type="password"/>
<input type="button" value="OK"/>	

Fig. 38: Network:PPPoE

■ PPPoE Login

In this field, enter the user name (Login), which is expected by your Internet Service Provider when you setup a connection to the Internet.

■ PPPoE Password

In this field, enter the password, which is expected by your Internet Service Provider when you setup a connection to the Internet.

6.5.4 Network:PPTP

Requirement: The RR-EPL has been set to the network mode PPTP (see “PPTP Mode” on page 74).
User name (Login) and password are requested by the Internet service provider (ISP), when you wish to establish a connection with the Internet.

Network > PPTP

PPTP Login	<input type="text" value="user@provider.example.net"/>
PPTP Password	<input type="password"/>
Local IP Mode	Static (from field below) ▼
Local IP	<input type="text" value="10.0.0.140"/>
Modem IP	<input type="text" value="10.0.0.138"/>
<input type="button" value="OK"/>	

Fig. 39: Network:PPTP

- **PPTP Login**
In this field, enter the user name (Login), which is expected by your Internet Service Provider when you setup a connection to the Internet.
- **PPTP Password**
In this field, enter the password, which is expected by your Internet Service Provider when you setup a connection to the Internet.

■ Set local IP

Via DHCP

If the address data for access to the PPTP server is supplied by the Internet service provider per DHCP, select `via DHCP`.

You do not have to make an entry under `Local IP`.

`Modem IP`. This is the address of the PPTP server of the Internet Service Provider.

`static` (following field)

If the address data for accessing the PPTP server is not supplied by the Internet service provider per DHCP, the IP address must be specified as a local IP address for the PPTP server.

`Local IP`. IP address, at which the RR-EPL can be reached from the PPTP server.

`Modem IP`. This is the address of the PPTP server of the Internet Service Provider.

6.5.5 Network:Extended Settings

■ **ARP Timeout**

Specify in seconds how long ARP waits for a response before the query is seen to have failed.

■ **MTU of the internal interface**

MTU (Maximum Transmission Unit) is the maximum length of an IP datagram.

Longest IP datagram that the internal interface accepts.

■ **MTU of the internal interface for VLAN**

Longest IP datagram that the internal interface accepts for VLANs.

■ **MTU of the external interface**

Longest IP datagram that the external interface accepts.

■ **MTU of the external interface for VLAN**

Longest IP datagram that the external interface accepts for VLANs.

■ **MTU of the management interface**

Longest IP datagram that the internal management interface accepts.

■ **MTU of the managementi Interface for VLAN**

Longest IP datagram that the internal management interface accepts for VLANs.

6.5.6 Network:Status

■ Network mode

Displays the current operating mode of the RR-EPL: router, PPPoE or PPTP (see “[Network:Base](#)” on page 72).

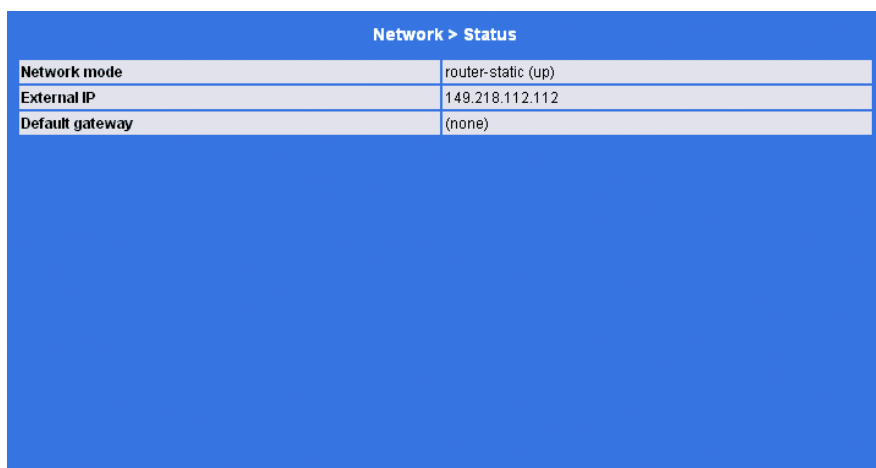
■ External IP

The IP address of the RR-EPL at its connection for the insecure network (WAN or Internet).

If the RR-EPL is assigned an IP address dynamically, you can look up the currently valid IP address here.

■ Default gateway

The default gateway address is shown here that is entered in the RR-EPL.



Network mode	router-static (up)
External IP	149.218.112.112
Default gateway	(none)

Fig. 40: Network:Status

6.6 Configuring the firewall

The RR-EPL contains a stateful packet inspection firewall. The connection data of an active connection are recorded in a database (referred to as connection tracking). Rules only need to be defined for one direction; data from the opposite direction of a connection and only this data is automatically passed through. A side effect is that existing connections are not interrupted during reconfiguration, even if a new connection can no longer be set up.

Factory settings for the firewall:

- ▶ All incoming connections will be accepted.
- ▶ The data packets of all outgoing connections will be passed through.

Note: VPN connections are not subject to the firewall rules defined under this menu item. You can define firewall rules for each individual VPN connection in the menu [“VPN:Connections” on page 98](#).

Note: If multiple firewall rules are set, they will be searched in the order in which they are listed (from top to bottom) until a suitable rule is found. This rule will then be applied. If further down in the list there are other rules, which would also fit, they will be ignored.

6.6.1 Firewall:Incoming

Lists the firewall rules that have been set. They apply to incoming data packets that are initiated externally.

Note: If no rule has been set, all incoming connections (except for VPN) are rejected.

Note: With the protocol setting “All”, the port settings are ignored.

Firewall > Incoming (untrusted port)								
	Protocol	From IP	From Port	To IP	To Port	Action	Comment	Log
<input type="checkbox"/>	All	0.0.0.0/0	any	0.0.0.0/0	any	Accept		No
Log entries for unknown connection attempts								No
OK								
These rules specify which traffic from the outside is allowed to pass to the inside. <i>Please note: Port settings are only meaningful for TCP and UDP</i>								

Fig. 41: Firewall:Incoming

■ Editing a rule

The following options are available:

- ▶ Protocol: `All` means: TCP, UDP, ICMP and other IP protocols.

Note: If you select `All`, the RR-EPL ignores the port settings (`from port`, `to port`).

- ▶ IP address: `0.0.0.0/0` means all addresses. To indicate a range, use the CIDR notation - see “[CIDR \(Classless InterDomain Routing\)](#)” on page 160.
- ▶ Port:
(is only evaluated for the protocols TCP and UDP)
`any` refers to any port.
`startport:endport` (e. g. `110:120`) refers to a port range.
Individual ports can be specified either with the port number or with the respective service name: (e. g. `110` for `pop3` or `pop3` for `110`). A list of the most commonly used port numbers can be found at <http://www.iana.org/assignments/port-numbers>.
- ▶ Action:
`Accept` means the data packets are permitted to pass through.
`Reject` means that the data packets are not accepted, and the sender is notified that the data was rejected. In transparent mode, `Reject` has the same effect as `Discard`.
`Discard` means the data packets are not permitted to pass through. They are discarded, and the sender is not notified about what happened to the data.

Note: In Transparent mode `Reject` is supported if the local IP address is entered correctly.

- ▶ Log
For each individual firewall rule you can decide if, when the rule is applied,
 - the event should be logged – set `Log` to `Yes`
 - or not – set `Log` to `No` (factory default setting).
- ▶ Log entries for unknown connection attempts
This logs all connection attempts that are not recorded by the preceding rules.

6.6.2 Firewall:Outgoing

Lists the firewall rules that have been established. They apply to outgoing data connections that are initiated internally. The default setting allows all packets to pass through.

With the default rule, all outgoing connections are permitted to pass through.

Note: With the protocol setting “All”, the port settings are ignored.

Protocol	From IP	From Port	To IP	To Port	Action	Comment	Log
All	0.0.0.0/0	any	0.0.0.0/0	any	Accept	default rule	No

Log entries for unknown connection attempts

OK

These rules specify which traffic from the inside is allowed to pass to the outside.
Please note: Port settings are only meaningful for TCP and UDP.

Fig. 42: Firewall:Outgoing

■ Editing a rule

The following options are available:

- ▶ Protocol: `All` means: TCP, UDP, ICMP, and other IP protocols.

Note: If you select `All`, the RR-EPL ignores the port settings (`from port`, `to port`).

- ▶ IP address: `0.0.0.0/0` means all addresses. To indicate a range, use the CIDR notation - see CIDR (Classless InterDomain Routing) - see [“CIDR \(Classless InterDomain Routing\)” on page 160](#).
- ▶ Port:
 - `any` refers to any port.
 - `startport:endport` (e. g. `110:120`) refers to a port range.
 - Individual ports can be specified either with the port number or with the respective service name: (e. g. `110` for `pop3` or `pop3` for `110`).
- ▶ Action:
 - `Accept` means the data packets are permitted to pass through.
 - `Reject` means that the data packets are not accepted, and the sender is notified that the data was rejected. In transparent mode, `Reject` has the same effect as `Discard`.
 - `Discard` means the data packets are not permitted to pass through. They are “swallowed”, and the sender is not notified about what happened to the data.

Note: In Transparent mode `Reject` is supported if the local IP address is entered correctly.

- ▶ Log
 - For each individual firewall rule you can decide if, when the rule is applied,
 - the event should be logged – set Log to `Yes`
 - or not – set Log to `No` (factory default setting).
- ▶ Log entries for unknown connection attempts
 - This logs all connection attempts that are not recorded by the preceding rules.

6.6.3 Firewall:Port Forwarding

Lists the rules that have been defined for port forwarding.

The following takes place when during port forwarding: The headers of the incoming data packets from the external network that are addressed to the external IP address (or to one of the external IP addresses) of the RR-EPL as well as to a specific port of the RR-EPL are translated in such a way that they are forwarded to the internal network to a particular computer and to a particular port of this computer. This means that the IP address and port number in the header of the incoming data packets are changed.

This procedure is also referred to as Destination NAT.

Note: These rules do apply in router mode.

Note: The rules established here have priority over the settings under [“Firewall:Incoming” on page 84](#).

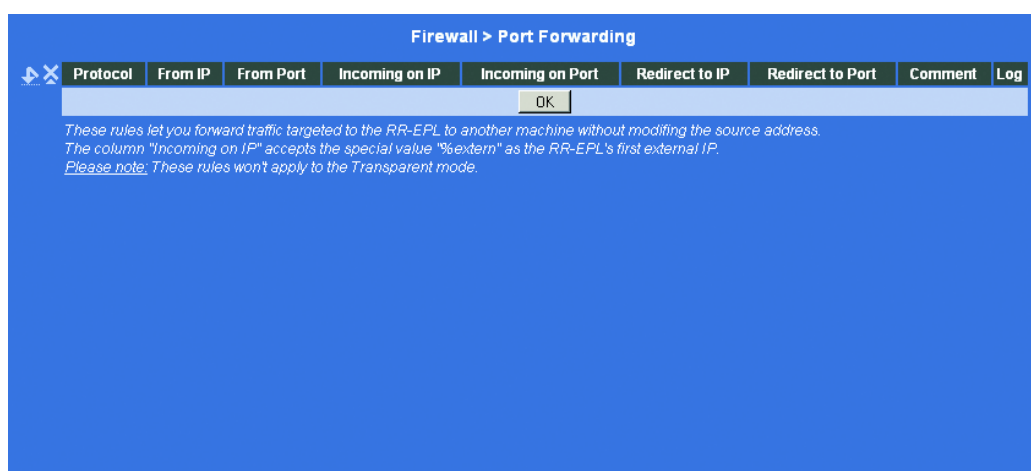


Fig. 43: Firewall:Port Forwarding

■ Editing a rule

The following options are available:

- ▶ Protocol
Enter the protocol which the rule is to refer to.
- ▶ From IP
Here you enter the source IP address from which the data packets come, to which you want to apply the rule.
- ▶ From Port
Here you enter the source port from which the data packets come, to which you want to apply the rule.
- ▶ Incoming for IP:
Enter the external IP address (or one of the external IP addresses) of the RR-EPL.
OR
In case there is a dynamic change of the external IP addresses of the RR-EPL so that you can enter the address, use the following variable:
`%external.`
- ▶ Incoming for port:
Original destination port that is specified in the incoming data packets.
- ▶ Forward to IP:
IP address to which data packets are to be forwarded and into which the original destination addresses are to be translated.
- ▶ Forward to port:
Port to which data packets are to be forwarded and into which the original port information is to be translated.
Ports can be specified either with the port number or with the respective service name: (e. g. 110 for pop3 or pop3 for 110).
- ▶ Log
For each individual port forwarding rule you can decide if, when the rule is applied,
 - the event should be logged – set Log to `Yes`
 - or not – set Log to `No` (factory default setting).

6.6.4 Firewall:NAT

For outgoing addresses the RR-EPL can translate the specified sender IP addresses from its internal network (in the example below: 192.168.x.x) into its own external address (in the example below: 148.218.112.7 or 149.218.112.8). The RR-EPL can break down the assignment of the incoming data packets using the logical ports.

This method is used if the internal addresses cannot or should not be routed externally, for example, because a private address range such as 192.168.x.x is being used or the internal network structure is to be concealed.

This procedure is also referred to as IP masquerading.

The dialog lists the defined rules for NAT (Network Address Translation).

■ Principle of IP masquerading

For addressing purposes, TCP/IP uses so-called port numbers (UDP, TCP) for the source and destination in addition to the IP addresses.

Masquerading makes use of this feature.

If the RR-EPL receives a data packet in router mode at a secure port, it will then enter the IP address of the sender (source) and the port in an internal table. The RR-EPL assigns this table entry its own IP port address and a random port number as new source information. The RR-EPL then forwards the data packet with this new information at the insecure port.

This is how the receiver sends its reply to this data packet to the RR-EPL. The RR-EPL in turn forwards the reply back to the original address using its internal address.

This method permits a communication request from the the secure to the insecure network, for example, for one computer located in cell 3 to a computer in the industrial backbone (see the figure below).

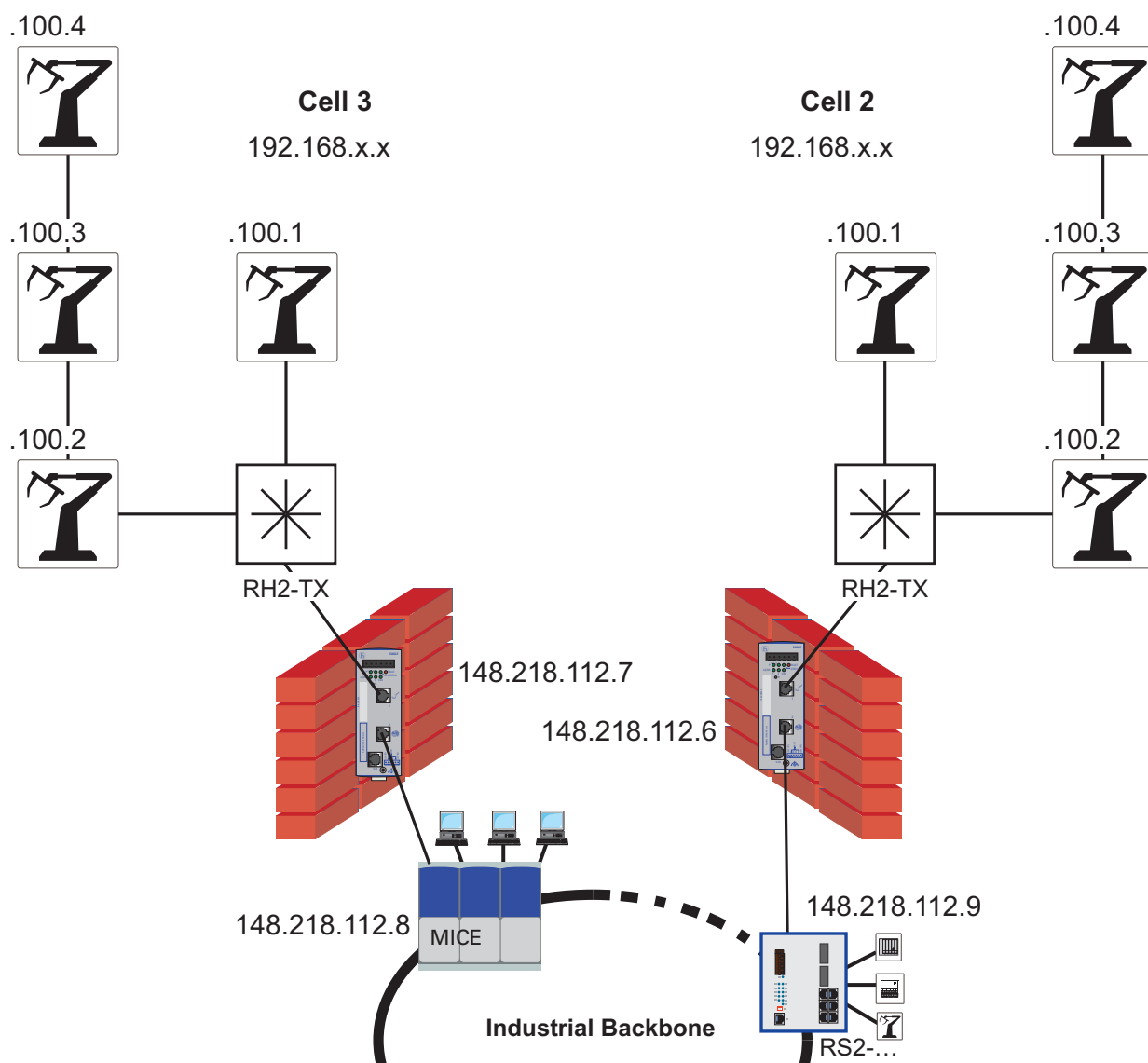


Fig. 44: Example of a masquerading application: two identically structured production cells

Note: If the RR-EPL is operating in PPPoE/PPTP mode, NAT must be activated to obtain access to the Internet. If NAT is not activated, only VPN connections can be used.

Factory setting: There is no NAT.



Fig. 45: Firewall:NAT

■ Editing a rule

The following entry options are available:

► From IP:

0.0.0.0/0 means all addresses. In other words, all internal IP addresses are subject to the NAT procedure. To indicate a range, use the CIDR notation - see [“CIDR \(Classless InterDomain Routing\)” on page 160](#).

Example:

For the IP address range 192.168.0.33 to 192.168.0.64 enter:
192.168.0.1.33/27.

6.6.5 Firewall:1-to-1 NAT

Bi-directional NAT is supported in pure router mode. A 1-to-1 conversion takes place here between IP addresses/subnetworks in the secure network and the defined IP addresses/subnetworks of the insecure IP interface. A typical 1-to-1 NAT application is the joining of two identical production cells (see Fig. 44). In contrast to IP masquerading, a communication request is possible here from both directions.

Note: The firewall rules are only applied after the addresses are converted. For this reason, you use the addresses that are actually present in the firewall rules.

Note: In RR-EPL Release 1.02 there is no ARP resolution for the converted IP addresses.

Cell 1 (secure network)	External network (unsecure network)	Cell 2 (unsecure network)	External network (unsecure network)
192.168.0.1/32	149.218.112.101/32	192.168.0.1/32	149.218.112.201/32
192.168.0.2/32	149.218.112.102/32	192.168.0.2/32	149.218.112.202/32
192.168.0.3/32	149.218.112.103/32	192.168.0.3/32	149.218.112.203/32
192.168.0.4/32	149.218.112.104/32	192.168.0.4/32	149.218.112.204/32

Table 7: Address translation table for the two RR-EPL (see Fig. 44)

- ☐ When you enter address ranges, enter the same address range for the internal and the external networks.
Example:
Secured network: 192.168.0.16/28
Unsecured network: 149.218.112.32/28

Firewall > 1:1 NAT

Local network	External network	Netmask
		OK

Please note: These rules won't apply to the Transparent mode.

Fig. 46: Firewall:1-to-1 NAT

6.6.6 Firewall:Extended Settings

The settings determine what the basic responses of the firewall will be.

Firewall > Extended Settings	
All Modes	
Maximum size of connection tracking table	4096
Maximum number of new outgoing TCP connections (SYN) per second	75
Maximum number of new incoming TCP connections (SYN) per second	25
Maximum number of outgoing "ping" frames (ICMP Echo Request) per second	5
Maximum number of incoming "ping" frames (ICMP Echo Request) per second	3
Enable "FTP" NAT/Connection Tracking support	Yes
Enable "IRC" NAT/Connection Tracking support	Yes
Enable "PPTP" NAT/Connection Tracking support	No
Enable TCP/UDP/ICMP consistency checks	Yes
Transparent Mode Only	
Maximum number of outgoing ARP requests or ARP replies per second (in each case)	500
Maximum number of incoming ARP requests or ARP replies per second (in each case)	500
Allow forwarding of GVRP frames	No
Allow forwarding of STP frames	No
Router Modes	
ICMP from extern to the EAGLE	Drop
OK	

Fig. 47: Firewall:Extended Settings

- ▶ **Maximum number of ...**
These 5 settings define upper limits. They are so selected that they are never reached in normal operation. However, since they can be easily reached in the event of an attack, the limits provide additional security. If your operational environment has special requirements, you can increase these values.
- ▶ **Enable "Active FTP" NAT/Connection Tracking support**
If an outgoing FTP (protocol) connection is setup to download data, the server called will callback the calling system to establish a connection for this transfer of data. In other words, for the calling client, the connection is simply an additional incoming connection, which will be setup with "Active FTP". In this case, Enable "Active FTP" NAT/Connection Tracking support must be set to Yes so that the firewall will pass the data through (factory setting). Without this function, the unit only permits passive FTP.

- ▶ Enable “IRC” NAT/Connection Tracking support
This is similar to “Active FTP”: When the IRC protocol is used for chatting in the Internet, incoming connections must also be permitted after the connection has been established actively. In this case, `Enable “IRC” NAT/Connection Tracking support` must be set to `Yes` so that the firewall will permit these connections (factory setting).
- ▶ Enable “PPTP” NAT/Connection Tracking support
This need only be set to `Yes` under the following condition:
if a local system should establish a VPN connection via PPTP to an external system without help from the RR-EPL.
The factory setting is `No`.
- ▶ ICMP from extern to RR-EPL
With this setting you can specify how the RR-EPL reacts to ICMP queries in the router mode:
`Drop`: the RR-EPL rejects incoming ICMP packets
`Allow ping requests`: the RR-EPL responds to ping queries.
`Allow all ICMPs`: the RR-EPL reacts to all ICMP packets.

6.6.7 Firewall:Logs - Display

If the logging of events was activated (`Log = Yes`) on the firewall rules page, you can view the log with all of the recorded events here.

The format of the log corresponds to that common under Linux.

Special analysis programs are available which can be used to present the information from the log in a more readable format.

6.7 Setting up a VPN connection

Prerequisites for a VPN connection:

The main prerequisite for a VPN connection is that the IP address of the VPN partner is known and accessible. See [“Services:DynDNS Monitoring” on page 120](#).

- ▶ To successfully set up an IPsec connection, the VPN remote terminal must support IPsec with the following configuration:

- ▶ Authentication via Pre-Shared Key (PSK) or X.509 certificate

Note: The Hirschmann Competence Center creates and manages safety certificates.

- ▶ ESP
 - ▶ Diffie-Hellman Groups 2 and 5
 - ▶ DES, 3DES or AES encryption
 - ▶ MD5 or SHA-1 hash algorithms
 - ▶ Tunnel or Transport mode
 - ▶ Quick Mode
 - ▶ Main Mode
 - ▶ SA Lifetime (1 second to 24 hours; standard: 8 hours)

If the system at the remote site is running Windows 2000, the Microsoft Windows 2000 High Encryption Pack or Service Pack 2 must also be installed.

- ▶ If the remote site is behind a NAT router, it must support NAT-T or the NAT router must support the IPsec protocol (IPsec/VPN Passthrough). In either case, for technical reasons, only IPsec Tunnel connections are supported.

6.7.1 VPN:Connections

Lists the VPN connections that have been setup.

All of the listed connections may be active at the same time.



Fig. 48: VPN:Connections

■ Setting up new a VPN connection

- ☐ Click “New”.
- ☐ Assign a name to the connection and click “Edit”.
- ☐ Make the desired or required settings (see below).
- ☐ Afterwards, click OK.

■ Editing the VPN connection

- ☐ Click the button “Edit” next to the respective connection.
- ☐ Make the desired or required settings (see below).
- ☐ Afterwards, click OK.

VPN > Connections > Connection (unnamed)

A descriptive name for the connection: [(unnamed)]

Enabled: [Yes]

Address of the remote site's VPN gateway (either an IP address, a hostname, or %any): [%any]

Authentication method: [X.509 Certificate] [Configure]

Connection type: [Transport (Host <-> Host)]

Connection startup (Will be ignored in Transparent Mode.): [Wait for connection from...] ...remote VPN gateway.

More IKE Options: [Configure]

Tunnel Settings

Local network address: [192.168.1.1]

The appropriate local netmask: [255.255.255.255]

The virtual IP which will be used by the client in Transparent mode: [192.168.1.1]

Remote network address: [192.168.254.1]

The appropriate remote netmask: [255.255.255.255]

Firewall Incoming (untrusted port)

Protocol	From IP	From Port	To IP	To Port	Action	Comment	Log
All	0.0.0.0/0	any	0.0.0.0/0	any	Accept	default rule - pleas	No

Fig. 49: VPN:Connections:Connection

■ Deleting a connection

- Click “Delete” next to the respective entry. Then “OK”.

■ Any name for the VPN connection

You can give the connection any name you wish.

■ Active

Determine if the connection is to be active (=Yes) or not (= No).

■ Address of the remote site's VPN gateway

- ▶ What is meant is the address of the access (gateway) to the private network in which the remote communication partner can be found (see Fig. 50).
- ▶ If you wish to have the RR-EPL actively initiate and setup the connection to the remote site or if the device is in Stealth mode, enter the IP address of the remote site here. The remote site must have a fixed and known IP address. Instead of entering an IP address, you can enter a hostname (i.e. a domain name in the URL syntax - `www.xyz.de`).

If the remote site's VPN gateway does not have a fixed and known IP address, you can use the DynDNS Service to simulate a fixed and known address. See [“Services: DynDNS Monitoring” on page 120](#).

- ▶ If the RR-EPL is ready to accept the connection that initiates and establishes a remote terminal active to the local RR-EPL with random IP address, then enter: `%any`
In this case, the local RR-EPL can be “called” by a remote site, which has been dynamically assigned its IP address (by the Internet Service Provider), i.e. which has an IP address that changes. In this scenario, you may only enter an IP address when this is the fixed and known IP address of the remote “calling” site.

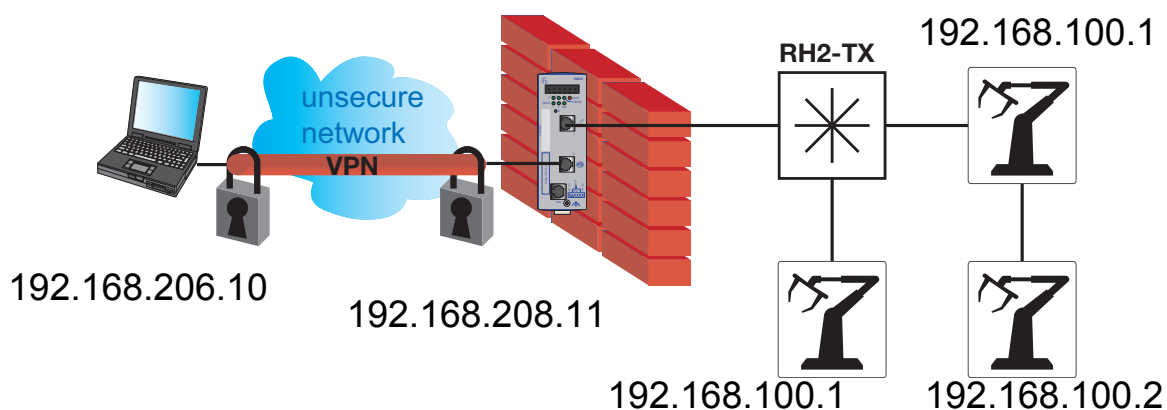


Fig. 50: Devices and addresses of the remote site

Dialog	Setting	Value
Network:Base	Internal IP	192.168.100.254
	Netmask	255.255.255.0
	Network Mode	Router
Network:Router	DHCP	No
	External IP	192.168.206.11
	Netmask	255.255.255.0
VPN:L2TP	Start L2TP Server for L2TP	Yes
	Local IP for L2TP connections	10.106.106.2
	Assignment of IPs for L2TP remote site	10.106.106.2
		10.106.106.254
VPN:Connections	Active	Yes
VPN:IPsec State	Gateway	192.168.206.11

Table 8: Example to devices and addresses of the remote site

■ Connection type

Connection type	annotation
Tunnels (Network <—> Network)	This type of connection is not only suitable in every case, but also the most secure. In this mode, the IP datagrams are completely encrypted before they are sent with a new header to the remote site's VPN gateway – the “tunnel end”. There the transferred datagrams are decrypted to restore the original datagrams. These are then passed on to the destination system.
Transport (Host <—> Host)	In this type of connection, the device only encrypts the data of the IP packets. The IP header information remains in the clear (unencrypted).
Transport (L2TP Microsoft Windows)	If this type of connection is activated on the remote system, the RR-EPL will also take this setting - Transport (L2TP Microsoft Windows) - and will function accordingly. In other words, the L2TP/PPP protocol will create a tunnel within the IPsec transport connection. The locally connected L2TP system will be assigned its IP address dynamically. If you select the connection type Transport (L2TP Microsoft Windows), set Perfect Forward Secrecy (PFS) to No (see below). As soon as the IPsec/L2TP connection is started under Windows, a dialog will appear to prompt you to enter your user name and password. You can make any entry that you want in this dialog, since the X.509 certificate has already provided your authentication, the RR-EPL will ignore these entries.
Transport (L2TP SSH Sentinel)	If this type of connection is activated on the locally connected system, the RR-EPL will also take this setting - Transport (L2TP SSH Sentinel) - and will function accordingly. In other words, the L2TP/PPP protocol will create a tunnel within the IPsec transport connection. The locally connected L2TP system will be assigned its IP address dynamically.

Table 9: Connections types

■ Initiating a connection

There are 2 options:

- Start a connection to the remote side
- Wait for the remote side [to setup a connection]

▶ Start a connection to the remote side

In this case, the local RR-EPL sets up the connection to the remote side. The fixed IP address or domain name of the remote side must be entered in Address of the remote site's VPN gateway (see above) field.

▶ Wait for the remote side [to setup a connection]

In this case, the local RR-EPL is ready to accept a connection, which a remote site actively initiates and sets up to the local RR-EPL.

The entry in the Address of the remote site's VPN gateway (see above) field may be: %any.

If the RR-EPL should only accept a connection initiated by a specific remote site (which has a fixed IP address), enter its IP address or hostname to be on the safe side.

■ Authentication method

There are 2 options:

- X.509 Certificate and
- Pre-Shared Key

► X.509 Certificate

This method is supported by most of the newer IPsec implementations and is currently considered the most secure. In this case, the RR-EPL uses the public key of the remote site (filename *.cer or *.pem) to encrypt the authentication datagram before it sends to the remote site, the “tunnel end”. (You must have received this *.cer or *.pem file from the operator at the remote site - perhaps on a diskette or attached to an e-mail).

To make this public key available to the RR-EPL, proceed as follows:
Requirement: You have saved the *.cer- or *.pem file on the computer.

- Click Configure.

Result: The screen VPN:connections:connection xyz:X.509 certificate appears. (“xyz” represents the name of the connection.)

- Search... click and select the file.
- Click Import.

After the import, the contents of the new certificate is displayed - see the following figure. For an explanation of the information displayed, see the Chapter [“VPN:Machine Certificate” on page 111](#).

VPN > Machine Certificate	
Certificate	No certificate & key installed
New Certificate	<div>PKCS#12 Filename (*.p12): <input type="text"/> <button>Durchsuchen...</button></div> <div>Password: <input type="password"/></div> <div><button>Import</button></div> <div><button>OK</button></div>

Fig. 51: Public key

► **Pre-Shared Key (PSK)**

This procedure is particularly supported by older IPsec implementations. Here, the RR-EPL encrypts the datagrams that it sends to the remote terminal, the “end of the tunnel”, with the public key of the remote terminal (filename *.cer or *.pem).

To make the arranged key available to the RR-EPL, proceed as follows:

– Click **Configure**.

Result: The main screen appears.

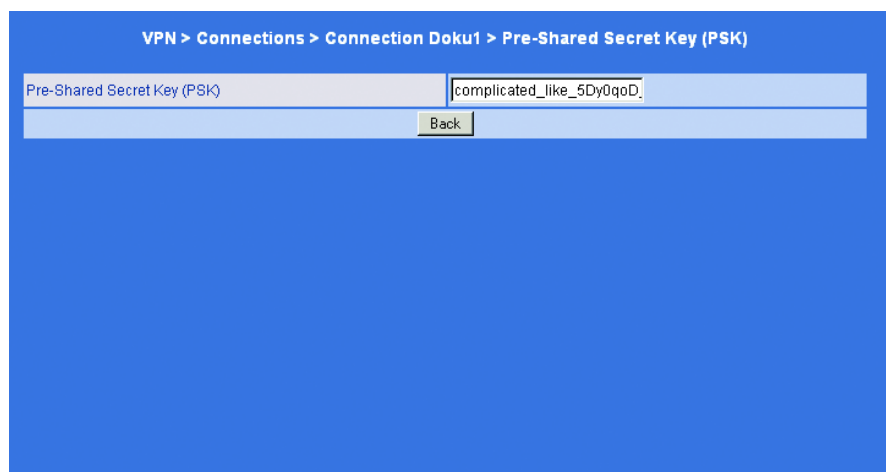


Fig. 52: Pre-Shared Secret Key

- Enter the string arranged in the entry field **Pre-Shared Key (PSK)**. To achieve a security level that is equivalent to 3DES, the string should be approx. 30 characters that are made up of upper and lower case letters and digits.
- Click **Back**.

Note: The **Pre-Shared Key** cannot be used with dynamic (%any) IP addresses; fixed IP addresses are required at both ends of the tunnel.

■ ISAKMP SA (key exchange)

- ▶ Encryption algorithm
 - Make arrangements with the administrator at the remote terminal as to which encryption procedure is to be used.3DES-168 is the most frequently used procedure and for this reason is the default setting.

The following principles apply: The more bits an encryption algorithm has, indicated by the number at the end, the higher level of security it offers. The relatively new procedure AES-256 is regarded as the most secure, but has not yet been widely implemented.

The encryption procedure takes longer, the longer the key is.

This aspect is irrelevant for the RR-EPL, since it operates with hardware-based encryption. This could, however, play a role for the remote terminal.

The algorithm named “Null” offers no encryption whatsoever.
- ▶ Checksum algorithm/Hash

Keep the setting on `All algorithms`. Then it makes no difference if the remote terminal operates with MD5 or SHA-1.

■ IPsec SA (data exchange)

In contrast to ISAKMP SA (key exchange) (see above), the procedure for exchanging data is defined here. It can differ from the keys of the key exchange, but this is not mandatory.

- ▶ Encryption algorithm

See above.
- ▶ Checksum algorithm/Hash

See above.

■ Perfect Forward Secrecy (PFS)

Procedure for increasing security in data transmissions. With IPsec the keys for exchanging data are renewed at specific intervals. With PFS new random numbers are negotiated with the remote station instead of deriving them from previously arranged random numbers.

Select **Yes** only if the remote terminal supports this procedure.

When you select the connection type **Transport (L2TP Microsoft Windows)**, set **Perfect Forward Secrecy (PFS)** to **No**.

■ Tunnel settings

- ▶ The address of the local network

- ▶ The related network mask

These entries specify the address of the client (network or computer), that is directly connected to the secure port of the RR-EPL which the RR-EPL is protecting. The address designates the local endpoint of the connection.

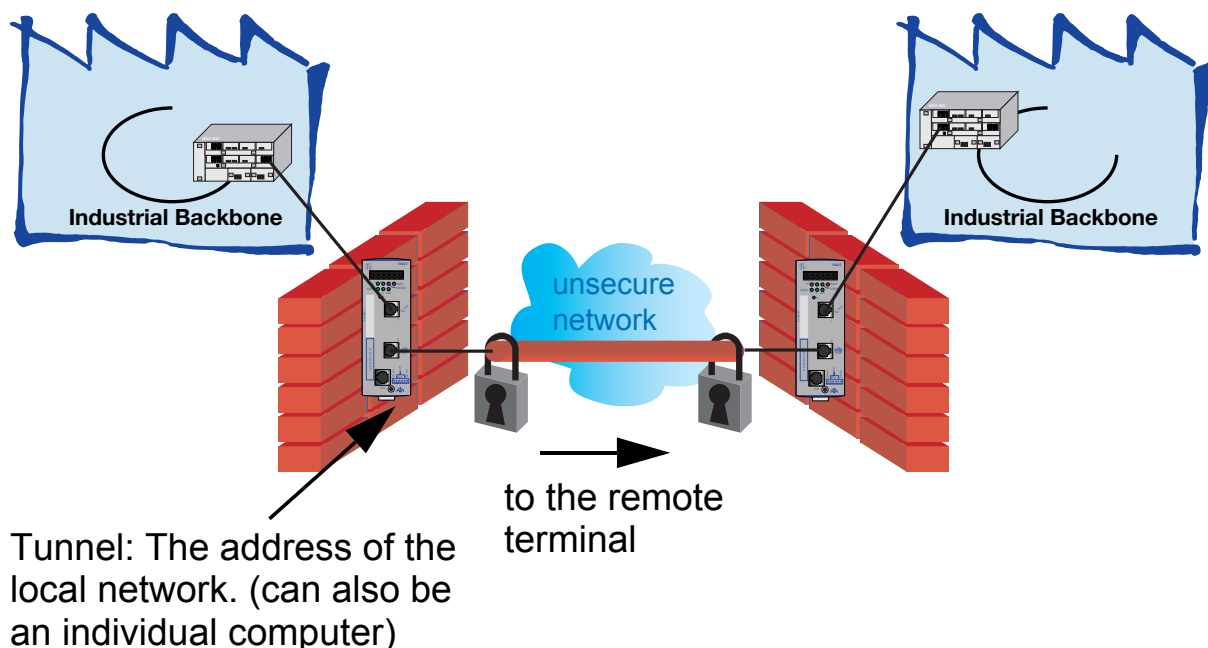


Fig. 53: Local devices and addresses

Example:

If the computer connected to the RR-EPL is the one you are using to configure the device, the entries could then be:

Address of the local network: 192.168.1.1

The related network mask: 255.255.255.0

See also [“Example of a network” on page 162](#).

- ▶ Tunnel: Remote network address
 - ▶ Tunnel: The appropriate remote netmask
- With these two entries, you specify the address of the network in which the remote communication partner can be found. This address can also be that of a computer, which is connected directly to the VPN gateway.

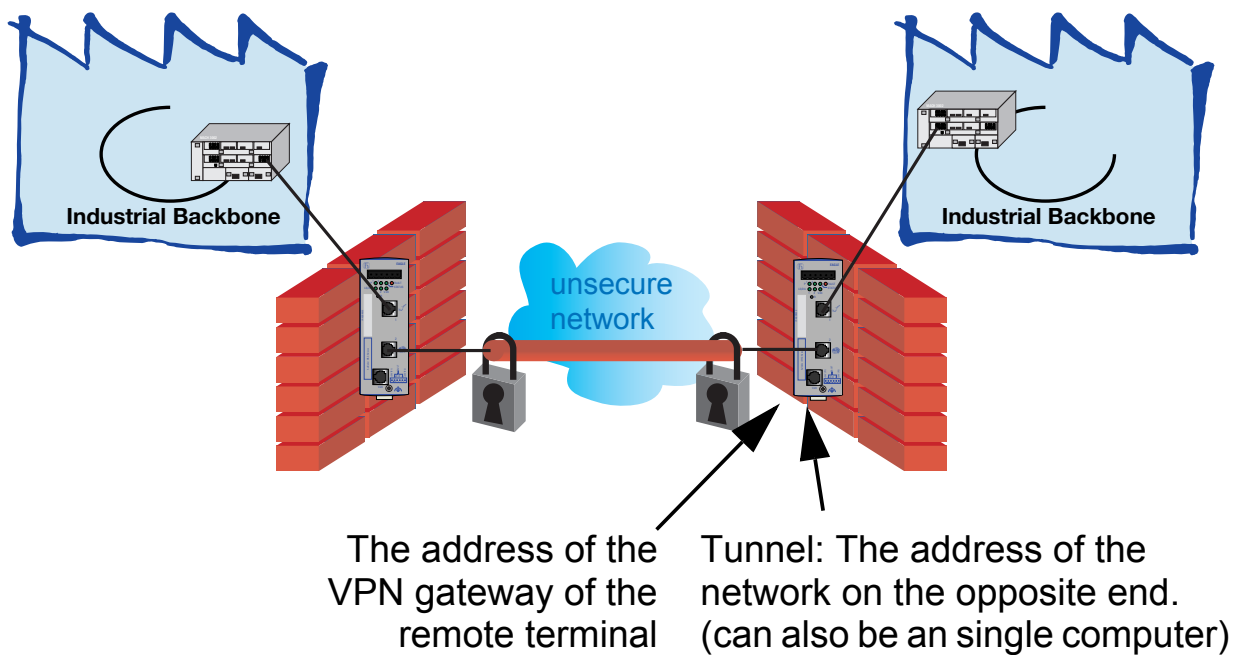


Fig. 54: Devices and address of the remote terminal

■ Firewall incoming, Firewall outgoing

While the settings made in the Firewall menu only affect non-VPN connections (see [“Firewall:Incoming” on page 84](#)), these settings affect just the VPN connection defined here. What this means is that: If you have defined multiple VPN connections, you can restrict the outgoing or incoming access individually for each connection. You can have any attempts made to bypass these restrictions logged.

Note: According to the factory setting, the VPN firewall is set up in such a way that everything is permitted for the VPN connection. The extended firewall settings, which are defined and explained at the top (see [“Firewall:Extended Settings” on page 95](#)), apply nonetheless for each individual VPN connection independent of each other.

Note: If multiple firewall rules are set, they will be searched in the order in which they are listed (from top to bottom) until a suitable rule is found. This rule will then be applied. If further down in the list there are other rules, which would also fit, they will be ignored.

- ☐ To set or delete a firewall rule, proceed as described in the earlier sections (see [“Firewall:Incoming” on page 84](#) and [“Firewall:Outgoing” on page 86](#)).

As there, you have the following entry options:

- ▶ Protocol: `All` means: TCP, UDP, ICMP and other IP protocols.
- ▶ IP address: `0.0.0.0/0` means all addresses. To enter an address space, use the CIDR notation (see [“CIDR \(Classless InterDomain Routing\)” on page 160](#)).
- ▶ Port: (is only evaluated for the protocols TCP and UDP)
`any` designates any port.
`startport:endport` (e. g. `110:120`) designates a port range.
Individual ports can be specified either with the port number or with the respective service name: (e. g. `110` for `pop3` or `pop3` for `110`).
- ▶ Action:
`Accept` means the data packets are permitted to pass through.
`Reject` means that the data packets are not accepted, and the sender is notified that the data was rejected. (In transparent mode, `Reject` has the same effect as `Discard`, see above)
`Discard` means the data packets are not permitted to pass through. They are “swallowed”, and the sender is not notified about what happened to the data.

Log

For each individual firewall rule you can decide if, when the rule is applied,

- the event should be logged – set Log to `Yes`
- or not – set Log to `No` (factory default setting).

Log entries for unknown connection attempts

If this is set to `Yes`, all attempts to establish a connection, which were not covered by the rules defined above, will be logged.

Note: In Transparent mode `Reject` is supported if the local IP address is entered correctly.

Note: If multiple firewall rules have been set, these will be processed in the order that they were entered.

6.7.2 VPN:Machine Certificate

VPN > Machine Certificate

Certificate	No certificate & key installed	
New Certificate	PKCS#12 Filename (*.p12):	<input type="text"/> <input type="button" value="Durchsuchen..."/>
	Password:	<input type="password"/>
	<input type="button" value="Import"/>	
<input type="button" value="OK"/>		

Fig. 55: Machine Certificate

■ Certificate

Display the currently imported X.509 certificate with which the RR-EPL identifies itself to other VPN gateways. The following information is displayed:

Info	Meaning
subject	The owner to whom the certificate is issued.
issuer	The point of authentication that signed the certificate. C : Country ST: State L : City O : Organization OU: Department (organization unit) CN: Hostname, common name
MD5, SHA1 Fingerprint	Fingerprint of the certificate so that it, for example, can be compared with others on the phone. Here, Windows displays the fingerprint in the SHA1 format.
notBefore, notAfter	Validity period of the certificate. Is ignored by the RR-EPL since it does not have a built-in clock.

Table 10: Certificate information

In addition to the information provided above, the imported certificate file (filename extension *.p12 or *.pfx) contains, both keys: the public key for encryption and the private one for decryption. The associated public key can be assigned to any number of connection partners, allowing them to send encrypted data.

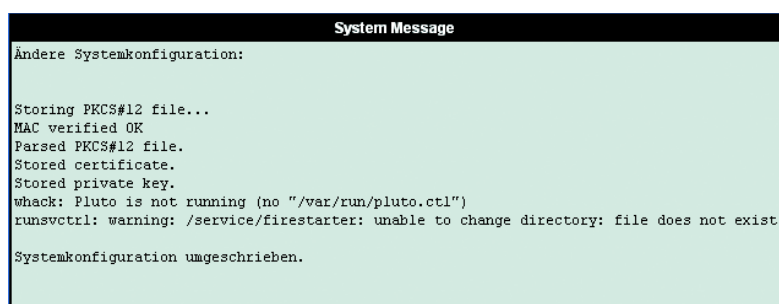
Dependant on the remote terminal, the certificate must be made available to the operator of the remote terminal as a .cer or .pem file - for example, by giving it to the operator personally or sending it as an e-mail. If you do not have access to a secure transmission path, you should compare the fingerprint displayed by the RR-EPL over a secure path. Only one certificate file (PKCS#12 file) can be imported into the device. To import a (new) certificate, proceed as follows:

■ New certificate

Requirement:

The certificate file (filename = *.p12 or *.pfx) is generated and stored on the connected computer.

- ☐ Click Search... to select the file.
- ☐ Enter the password with which the private key of the PKCS#12 file is protected into the field.
- ☐ Click Import.
- ☐ Afterwards, click OK.
- ☐ After the import a system message will appear:



```
System Message
Andere Systemkonfiguration:

Storing PKCS#12 file...
MAC verified OK
Parsed PKCS#12 file.
Stored certificate.
Stored private key.
whack: Pluto is not running (no "/var/run/pluto.ctl")
runsvctrl: warning: /service/firestarter: unable to change directory: file does not exist

Systemkonfiguration umgeschrieben.
```

Fig. 56: System message

6.7.3 VPN:L2TP



Fig. 57: VPN:L2TP

■ **Start L2TP Server for IPsec/L2TP? Yes / No**

If you wish to permit an L2TP connection, set this switch to **Yes**. Within the IPsec transport connection, the L2TP connection contains in turn a PPP connection. This results in a type of tunnel between two networks. In doing so, the RR-EPL informs the remote terminal about the addresses that are used: for itself and for the remote terminal.

■ **Local IP for L2TP connections**

With the setting shown in the screenshot above, the RR-EPL will inform the remote site that it's address is 10.106.106.1.

■ **Assignment of IPs for the L2TP remote site**

With the settings shown in the screenshot above, the RR-EPL will inform the remote site that it has been assigned addresses starting from 10.106.206.2 (in the case of a single system) all the way to 10.106.206.254 (in the case of multiple systems).

6.7.4 VPN Configuration, IPsec Status - Display

Provides information about the status of the IPsec connections.

The names of the VPN connections are listed on the left. Their current statuses are displayed on their right.

- ▶ GATEWAY designates the communicating VPN gateways
- ▶ TRAFFIC designates the computers or networks that communicate via VPN gateways.
- ▶ ID designates the distinguished name (DN) of a X.509 certificate.
- ▶ ISAKMP status (Internet Security Association and Key Management Protocol) has the value “established”, if both participating VPN gateways have set up a channel for exchanging keys. In this case, they can contact each other and thus all entries, including “ISAKMP SA” on the configuration end of the connection were correct.
- ▶ IPsec status has the value “established”, if the IPsec encryption is activated for communication. In this case, the values under “IPsec SA” and “Tunnel Settings” were also correct.

Should you encounter problems, we recommend that you take a look at the VPN logs of the computer to which the connection was set up. For security reasons, the initiating computer will not be sent any detailed error messages.

If the display shows:

```
ISAKMP SA established, IPsec State: WAITING
```

This means that:

The authentication was successful, but the other parameters are not correct.

Do the connection types (Tunnel, Transport) match?

If Tunnel has been selected, do the network address areas match on at both ends of the connection?

If the display shows:

```
IPsec State: IPsec SA established
```

This means that:

The VPN connection has been successfully setup and can be used. If this is not the case, there must be a problem with the remote VPN gateway. In this case, click on the connection name and then on OK to setup the connection again.

6.7.5 VPN:L2TP Status - Display

Shows information about the L2TP status, when this type of connection has been selected. See [“VPN:L2TP” on page 114](#)).

6.7.6 VPN:VPN Logs - Display

Lists all VPN events.

The format of the log corresponds to that common under Linux.

Special analysis programs are available which can be used to present the information from the log in a more readable format.

6.8 Services menu

6.8.1 Services:DNS

If the RR-EPL is to set up a connection to a remote terminal (for example VPN gateway or NTP server), it must know the IP address of the remote terminal. If the address is provided as a domain address (i. e. in the format `www.abc.xyz.de`), the device must first look up which IP address this resolves to on the domain nameserver.

If the RR-EPL is not in transparent mode, you can configure the locally connected clients, so that they can use the RR-EPL to resolve the hostnames into IP addresses (see [“IP configuration for the Windows clients” on page 127](#)).

Services > DNS

Hostname mode	User defined (from field below) ▼
Hostname	EAGLE
Domain search path	example.local

In Transparent Mode, only "User defined" and "DNS Root Servers" are supported. Other settings will be ignored.

Servers to query	DNS Root Servers ▼
User defined name servers	IP

OK

Fig. 58: Services:DNS

■ **Hostname mode**

With `hostname mode` and `hostname` you can assign the RR-EPL a name. It will be displayed when someone logs in with SSH. A name environment simplifies the administration of several RR-EPLs.

- ▶ User defined (see below)
(Standard) The name entered in the field `hostname` is set as the name for the RR-EPL.

Note: If the RR-EPL is operating in transparent mode, the option `User defined` must be selected as the `hostname mode`.

- ▶ Provider defined (e. g. via DHCP)
If the network mode permits the hostname to be set externally, such as with DHCP, the name transmitted by the provider will then be set for the RR-EPL.

■ **Hostname**

If the option `User defined` is selected under `hostname mode`, then enter the name here that is to be given to the RR-EPL.

If the option `Provider` (e. g. via DHCP) is selected under `Hostname mode`, an entry in this field will be ignored.

■ **Domain search path**

This entry make it easier for the user to specify a domain name: If the user enters the domain name in an abbreviated form, the RR-EPL will extend the entry by appending the domain suffix, which is defined here in the `Domain search path`.

■ **Used nameserver**

Options:

- Root Nameserver
- Provider defined
- User defined

- ▶ **Root Nameserver**
Requests are sent to the root nameserver in the Internet whose IP addresses are stored in the RR-EPL. These addresses seldom change. This setting should only be selected if the alternative settings do not function.
- ▶ **Provider defined**
With this setting, the device will use the Domain nameserver of the Internet Service Provider, which is used to access the Internet. You can select this setting, when the RR-EPL will be operated in PPPoE or Router mode with DHCP active (see [“Services:DHCP Intern \(trusted port\)” on page 123](#)).
- ▶ **User defined**
If this setting is selected, the RR-EPL sets up a connections with the domain nameservers that are listed in `User-defined nameserver`. In transparent mode only the first two entries are evaluated in this list.

■ **User defined nameservers**

You can record the IP addresses of domain nameservers in this list. If one of these should be used by the RR-EPL, specify this under `Servers to query`.

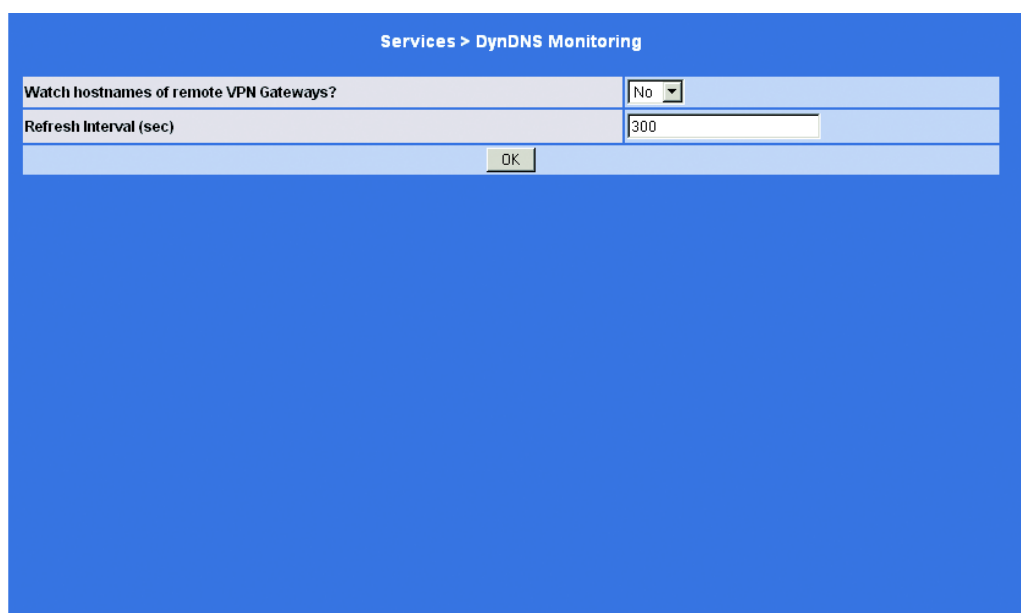
Note: If you have selected User defined, you must configure the locally connected clients to use the address of the RR-EPL to retrieve the IP address associated with a hostname (see [“IP configuration for the Windows clients” on page 127](#)).

6.8.2 Services: DynDNS Monitoring

When setting up aVPN connection between two locations, it is assumed that the IP address of at least one location is known and thus can be defined. Many Internet service providers (ISP) assign IP addresses dynamically. This means that the IP addresses of the computers or networks that access the Internet always change.

To solve the problem of assigning IP address dynamically, so-called DynDNS services can be used. Such a service makes it possible for the RR-EPL to reach a fixed domain name regardless of the IP address it is currently using. Each time the IP address changes, the RR-EPL reports the new IP address to the DynDNS server so that the current IP address is always correctly assigned to the domain name on the DNS server (see [“Glossar” on page 195](#)).

For further information, contact Hirschmann support.



The screenshot shows a web-based configuration window titled "Services > DynDNS Monitoring". It contains two input fields: "Watch hostnames of remote VPN Gateways?" with a dropdown menu set to "No", and "Refresh Interval (sec)" with a text input field containing "300". Below these fields is an "OK" button. The background of the window is blue.

Fig. 59: DynDNS monitoring

■ Monitoring hostnames from VPN remote terminals

If the address of the VPN remote terminal is specified to the RR-EPL as the hostname (see [“VPN:Connections” on page 98](#)), and if this domain name is assigned by a DynDNS service, then the RR-EPL can poll if changes have been made at the respective DynDNS.

■ Polling interval

Standard: 300 (seconds)

6.8.3 Services: DynDNS registration

To set up VPN connections at least the IP address of one of the partners must be known, so that the partners can communicate with each other. This is not case if both participants are assigned IP addresses dynamically from their Internet service providers. In such a case, a DynDNS service, such as the one from the Hirschmann Competence Center or DNS4BIZ.com can help. With the DynSNS service, the currently valid IP address is registered under a fixed name (see [“Services: DynDNS registration” on page 121](#)).

Provided that you are registered for one of the DynDNS services supported by the RR-EPL, you can make the proper entries in the dialog box.

Services > DynDNS Registration	
Register this EAGLE at a DynDNS Service?	No
Refresh Interval (sec)	420
DynDNS Provider	DynDNS.org
DynDNS Server	dyn.hirschmann.de
DynDNS Login	
DynDNS Password	
DynDNS hostname	host.example.com
OK	

Fig. 60: DynDNS registration

■ Register this RR-EPL at a DynDNS Service?

Select **Yes**, if you have registered with a DynDNS Service provider and the RR-EPL should utilize this service. In this case, the RR-EPL will report its current IP address - the one assigned for its own Internet access by its Internet Service Provider - to the DynDNS Service.

■ Refresh Interval

Standard: 420 (seconds)

Whenever the IP address of its own Internet access is changed, the RR-EPL will inform the DynDNS Service of its new IP address. For additional reliability, the device will also report its IP address at the interval set here.

■ DynDNS provider

The providers made available for selection support the same protocol that the RR-EPL supports.

Enter the name of the provider where you are registered, for example DynDNS.org.

■ DynDNS server

Name of the server of the DynDNS providers selected above, for example: dyndns.org.

■ DynDNS Login

Enter the user name that you have been assigned here.

■ DynDNS Password

Enter the password that you have been assigned here.

■ DynDNS Hostname

The hostname selected at DynDNS service for this RR-EPL- provided that you use a DynDNS service and have made the proper settings above.

6.8.4 Services:DHCP Intern (trusted port)

DHCP Internal has three operating modes:

- ▶ Deactivated:
DHCP is switched off at this port.
- ▶ Server:
The DHCP server (Dynamic Host Configuration Protocol) of the RR-EPL assigns the clients connected to the RR-EPL automatically
 - ▶ the IP addressed defined in the DHCP range and subnet masks or
 - ▶ the statically entered IP addresses.

Note: It is possible to configure the RR-EPL as a DHCP client in router mode (see [“External interface” on page 76](#)).

Option:

If the DHCP server is activated, you can enter the network parameters to be used by the clients during dynamic assignment:

Parameter	Meaning
Enable dynamic IP address pool	If no static assignment applies, then the RR-EPL assigns an IP address from the dynamic address pool.
DHCP lease time	Time in seconds after which the assigned IP address becomes invalid and the client makes a new DHCP query.
DHCP range start DHCP range end:	Beginning and end of the address range from which the DHCP server of the RR-EPL is to assign IP addresses to the locally connected clients.
Local netmask:	The default setting is: 255.255.255.0
Broadcast address	Specifies the broadcast address of the client.

Table 11: Client network parameters

Parameter	Meaning
Default gateway:	Determines which IP address for the client is to be used as the standard gateway.
DNS server:	Determines from where the clients are to obtain the IP addresses resolved from hostnames. If the DNS service of the RR-EPL is activated, this can be the local IP address of the RR-EPL.
WINS server	The Windows Internet Name Service determines from where the clients obtain the resolution of NetBIOS names in IP addresses.

Table 11: Client network parameters

Note: Only one DHCP server per subnet may be used.

Note: When you start the DHCP server of the RR-EPL, you must configure the locally connected clients in such a way that they automatically obtain their IP addresses.

- ☐ Set this switch DHCP mode to `Server`, if you wish to activate this function.
- ☐ Enter the parameters for the dynamic address assignment ([see Table 11 on page 123](#)) or enter the static MAC IP address assignment.
If you enter static addresses, then static addresses are assigned, otherwise dynamic ones.

► Relay

The static IP address assignment via the classic DHCP protocol is based on the device to be configured, which means that a particular IP address is assigned to the MAC address of a known device.

The static IP address assignment via Option 82 is based on the network topology. This procedure gives you the option of always assigning a particular IP address to any device which is connected to a particular location (port of a switch) on the LAN. The RR-EPL can take over the function of a DHCP relay agent. If this function is activated, then what is known as an Option 82 field is added to the DHCP query if the query does not already have an Option 82 field. The Option 82 field contains information about the switch (port, device ID) to which the querying device is connected.

- ☐ Enter the IP addresses of the DHCP server to which you want to forward DHCP queries.
- ☐ You switch on the DHCP relay option by setting “Append Relay Agent Information (Option 82)” to “Yes”.

Services > DHCP Intern (trusted port)

DHCP mode	Disabled				
DHCP Server Options					
Enable dynamic IP address pool	No				
DHCP lease time	3600				
DHCP range start	192.168.1.100				
DHCP range end	192.168.1.199				
Local netmask	255.255.255.0				
Broadcast address	10.0.0.255				
Default gateway	192.168.1.1				
DNS server	10.0.0.254				
WINS server	10.0.0.254				
Static Mapping	<table border="1"> <thead> <tr> <th>Client MAC Address</th> <th>Client IP Address</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> </tr> </tbody> </table>	Client MAC Address	Client IP Address		
Client MAC Address	Client IP Address				
DHCP Relay Options					
DHCP Servers to relay to	IP				
Append Relay Agent Information (Option 82)	No				
OK					

Statically entered MAC/IP address pairs

Fig. 61: Services:DHCP

6.8.5 Services:DHCP Extern (untrusted port)

DHCP External has three operating modes:

- ▶ Deactivated:
DHCP is switched off at this port.
- ▶ Server:
The DHCP server (Dynamic Host Configuration Protocol) of the RR-EPL assigns the clients connected to the RR-EPL automatically
 - ▶ the IP addressed defined in the DHCP range and subnet masks or
 - ▶ the statically entered IP addresses.

Note: It is possible to configure the RR-EPL as a DHCP client in router mode (see [“External interface” on page 76](#)).

Option:

If the DHCP server is activated, you can enter the network parameters to be used by the clients during dynamic assignment:

Parameter	Meaning
Enable dynamic IP address pool	If no static assignment applies, then the RR-EPL assigns an IP address from the dynamic address pool.
DHCP lease time	Time in seconds after which the assigned IP address becomes invalid and the client makes a new DHCP query.
DHCP range start DHCP range end:	Beginning and end of the address range from which the DHCP server of the RR-EPL is to assign IP addresses to the locally connected clients.
Local netmask:	The default setting is: 255.255.255.0
Broadcast address	
Default gateway:	Determines which IP address for the client is to be used as the standard gateway.
DNS server:	Determines from where the clients are to obtain the IP addresses resolved from hostnames. If the DNS service of the RR-EPL is activated, this can be the local IP address of the RR-EPL.
WINS server	The Windows Internet Name Service determines from where the clients obtain the resolution of NetBIOS names in IP addresses.

Table 12: Client network parameters

Note: Only one DHCP server per subnet may be used.

- ☐ Set the switch „DHCP mode“ to Yes, if you wish to activate this function.
- ☐ Enter the parameters for the dynamic address assignment ([see Table 11 on page 123](#)) or enter the static MAC IP address assignment.
If you enter static addresses, then static addresses are assigned, otherwise dynamic ones.

► **Relay**

The static IP address assignment via the classic DHCP protocol is based on the device to be configured, which means that a particular IP address is assigned to the MAC address of a known device.

The static IP address assignment via Option 82 is based on the network topology. This procedure gives you the option of always assigning a particular IP address to any device which is connected to a particular location (port of a switch) on the LAN. The RR-EPL can take over the

function of a DHCP relay agent. If this function is activated, then what is known as an Option 82 field is added to the DHCP query if the query does not already have an Option 82 field. The Option 82 field contains information about the switch (port, device ID) to which the querying device is connected.

- ☐ Enter the IP addresses of the DHCP server to which you want to forward DHCP queries.
- ☐ You switch on the DHCP relay option by setting “Append Relay Agent Information (Option 82)” to “Yes”.

■ **External server (untrusted port)**

- ☐ Set the Start DHCP server switch to `on`, to activate this function.
- ☐ Enter the parameters for the dynamic address assignment (see [Table 11 on page 123](#)) or enter the static MAC IP address assignment.

■ **IP configuration for the Windows clients**

In Windows XP, proceed by clicking

`Start:Control Panel:Network Connections`,

Right-click the LAN adapter icon and select `Properties` in the context menu.

In the dialog box `Properties of LAN connection Local Network` on the tab `General` under “Components checked are used by this connection”, select the entry `Internet protocol (TCP/IP)` and then click the button `Properties`.

In the dialog box `Internet Protocol (TCP/IP Properties)` select the option `Obtain an IP address automatically`.

6.8.6 Services:LLDP

IEEE 802.1AB describes the Link Layer Discovery Protocol (LLDP). LLDP enables the user to have automatic topology recognition for his LAN.

A device with active LLDP

- ▶ Distributes its connection and management information to the neighboring devices of the shared LAN, once these devices have also activated LLDP.
 - ▶ Receives connection and management information from neighboring devices of the shared LAN, once these devices have also activated LLDP.
 - ▶ Sets up a management information schema and object definition for saving connection information of neighboring devices with active LLDP.
- ☐ Use the “Mode” switch to switch on the LLDP function.
 - ☐ Set the LLDP parameters separately for each
 - secure area port and
 - insecure area port.

Parameter	Meaning
Mode	Switch LLDP function on/off.
Chassis ID	In Hirschmann devices, the device ID corresponds to the MAC address.
Port description	Port description that the RR-EPL adds to its LLDP information.
System name	The system name of the connected device.

Table 13: LLDP parameters

6.8.7 Services:NTP

The network time protocol (NTP) allows you to synchronize the system time within your network. NTP has a hierarchical structure. The NTP server makes the UTC (Universal Time Coordinated) available. The NTP client obtains the UTC from the SNTP server.

Services > NTP	
Current system time (UTC)	Sat Jan 1 02:17:56 UTC 2000
Current system time (local)	Sat Jan 1 02:17:56 UTC 2000
NTP State	(disabled)
Enable NTP time synchronization	No
NTP servers to synchronize to	NTP Server
Timezone in POSIX.1 notation (Eg. "CET-1" for the EU or "CET-1CEST,M3.5.0,M10.5.0/3" with automatic daylight saving time switching)	UTC
Time stamp in filesystem (2h granularity)	No
OK	

Fig. 62: Network time protocol

■ Current system time (UTC)

Displays the current system time in Universal Time Coordinates (UTC). If the `Enable NTP time synchronisation` not yet activated (see below) and `Time stamp in filesystem` is deactivated, the clock will start with 1 January 2000.

■ Current system time (local time)

If the possibly differing current local time should be displayed, you must make the corresponding entry under `Timezone` in POSIX.1 notation... (see below).

■ **NTP State**

Displays the current NTP state.

■ **Enable NTP time synchronization: Yes / No**

Once the NTP is enabled, the RR-EPL takes the time from the Internet and displays this as its current system time. The synchronisation can take several seconds.

If this option is set to `Yes` and at least one time server is specified under `NTP servers to synchronize to` (see below), the current system time will be made available.

■ **NTP servers to synchronize to**

Under this option, enter one or more time servers from which the RR-EPL should obtain the current time. If you enter multiple time servers, the RR-EPL will automatically connect with all of them to determine the current time.

Note: If you enter a hostname, e.g. `pool.ntp.org`, instead of an IP address, a DNS server must also be specified (see [“Services:DNS” on page 117](#)).

Note: If the RR-EPL is operating in Transparent mode and multiple time servers are entered, the RR-EPL will only use the first two time servers in the list.

Note: If the RR-EPL is operating in Router, PPPoE or PPTP mode, it will also make the NTP time available to the connected systems.

■ **Timezone in POSIX.1 Notation...**

If the `Current system time` above should display your current local time instead of the current Greenwich time (if it is different to the Greenwich time), you must enter the number of hours (plus or minus) that your local time differs from Greenwich time.

Examples:

In Berlin, the time is one hour earlier than in Greenwich. Therefore, enter: `CET-1`.

In the entry, the characters preceding the -1, -2 or +1 etc. are not considered. Only the numerical difference is important. The characters preceding the numerical difference may be "CET" or any other acronym that you find useful.

If you wish to display Central European Time (for example for Germany) and have it automatically switch to/from daylight saving time, enter:
CET-1CEST,M3.5.0,M10.5.0/3

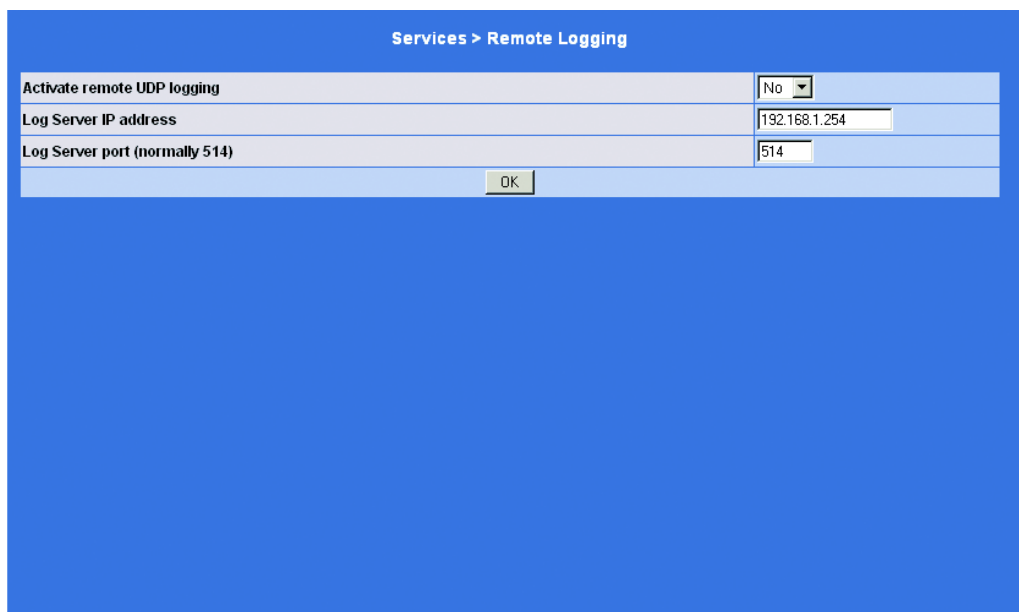
■ **Time stamp in filesystem (2h granularity): Yes / No**

If this option is set to Yes, the RR-EPL will save the current system time to its memory every two hours.

Afterwards: If the RR-EPL is switched off and back on, a time from this two hour period of time will be displayed when the RR-EPL is switched on and not (the factory setting) a time on 1 January 2000.

6.8.8 Services:Remote Logging

All log entries are recorded in the RR-EPL's memory. Once the memory available for the log has been filled, the oldest log entry will be overwritten. Furthermore, if the RR-EPL is switched off all log entries are deleted. If you wish to keep a copy of the log, the log entries can be sent to an external system. This is particularly useful if you wish to have centralised administration of the logs.



Services > Remote Logging

Activate remote UDP logging	No
Log Server IP address	192.168.1.254
Log Server port (normally 514)	514

OK

Fig. 63: Remote Logging

■ **Activate remote UDP Logging: Yes / No**

If all log entries should be sent to an external (specified below) Log Server, set this option to *Yes*.

■ **Log Server IP address**

Enter the IP address of the log server to which the log entries should be sent via UDP.

Note: This entry must be an IP address - not a hostname! This function does not support hostnames, since, if it did, it would not be possible to log the loss of a DNS server.

■ **Log Server port**

Enter the port of the log server to which the log entries should be sent via UDP. Standard: 514.

6.8.9 Services:SNMP Traps

This dialog allows you to determine which events trigger an alarm (trap) and where these alarms should be sent.

In the state on delivery, all the alarms are selected (does not apply for an update) .

When you switch on the SNMPv3 or SNMPv1/2 (see [“Access:SNMP” on page 145](#)) and define SNMP trap destinations (see below), the RR-EPL can send the selected traps.

Services > SNMP Traps

Basic traps

Enable SNMP authentication traps	Yes
Enable link Up/Down traps	Yes
Enable coldstart traps	Yes
Enable admin access (SSH, HTTPS) traps and DHCP new client traps	Yes

Hardware related traps

Enable chassis (power, signal relay) traps	Yes
Enable agent (ACA, temperature) traps	Yes

Anti-Virus related traps

Enable trap at (successful) update of AV pattern	Yes
Enable trap at update or scanning problems of AV components	Yes
Enable trap at found virus or skipped scanning	Yes

SNMP Trap Destinations

Destination IP	Destination Name	Destination Community
OK		

Platform-specific configurations are only effective on the platform in question.
Similarly AV traps are only sent when a licensed anti-virus system is active.
SNMP-traps only are sent if SNMP access is enabled.

Fig. 64: SNMP traps

■ Enable Authentication traps

The RR-EPL sends an authentication alarm, if it rejects an unauthorized access.

■ Enable link Up/Down traps

The RR-EPL sends a link status alarm if the connection to the connected network has been interrupted or re-established.

■ **Enable coldstart traps**

The RR-EPL sends a cold reset alarm after it has been switched on.

■ **Enable Admin traps**

The RR-EPL sends a SecurityGateway alarm if one of the following events has occurred:

- HTTPS login: There was a login attempt via HTTPS.
- Shell login: There was a login attempt via the shell.
- DHCP NewClient: The DHCP server has received a request from an unidentified client.

■ **Enable chassis traps**

The RR-EPL sends a chassis alarm if one of the following events has occurred:

- Power Supply: The status of a supply voltage has changed.
- Signaling relay: The status of the signal contact has changed.

■ **Enable agent traps**

The RR-EPL sends an agent alarm if one of the following events has occurred:

- Temperature: The temperature has exceeded / fallen below the set threshold values.
- AutoConfigAdapter: The Auto Configuration adapter, ACA, has been added or removed.

■ **Activate traps when virus search patterns have been updated (successfully)**

The RR-EPL sends an update alarm when the virus search patterns have been updated successfully.

■ Activate traps if there are update or virus scan problems

The RR-EPL sends a problem alarm if problems occur

- when updating virus search patterns or
- during virus scanning.

■ Activate traps if a virus is found or files are not checked

The RR-EPL sends a virus alarm if

- a virus was detected or
- a file was not checked.

■ SNMP trap destinations

`Destination IP`: Enter the IP address of the recipient here, to which the traps are to be sent.

`Destination name`: Here you can enter a name of your choice for each recipient.

`Destination community`: The community with which the RR-EPL sends a trap. Enter the community here that the trap recipient is expecting.

6.9 Access menu

6.9.1 Access:passwords

The RR-EPL supports 3 levels of user authorization. To login at a specific level of authorization, the user must enter the corresponding password for the level.

Access > Passwords

Root Password (Account: root)	Old Password: <input type="text"/>
	New Password: <input type="text"/>
	New Password (again): <input type="text"/>
Administrator Password (Account: admin)	<input type="text"/>
	<input type="text"/>
Enable User Password	No <input type="button" value="v"/>
User Password	<input type="text"/>
	<input type="text"/>
<input type="button" value="OK"/>	

Fig. 65: Access:Password

■ Authorization level root

Offers all rights for all parameters of the RR-EPL.

Note: Only this authorization level allows you to connect to the device via SSH so that you can render the entire system useless by making faulty configurations. The system can then only be returned to its delivery state by flashing the firmware (see [“Flashing the firmware” on page 168](#)).

Default root password: `root`

To change the password, proceed as follows:

- ☐ Enter the currently valid root password in the field `Old Password`.
- ☐ Enter the new password twice in the fields `New Password` and `New Password (Repeat)`.

■ **Authorization level Administrator**

If you login at this level (password), you will be granted all the rights required for the configuration options that are accessible via the Web-based Administrator interface.

Default user name: `admin`

Default password: `private`

The user name `admin` cannot be changed.

To change the password, enter the desired new password twice in each of the corresponding entry fields.

■ **Authorization level User**

If a user password has been defined and activated, the user must - after every restart of the RR-EPL - enter this password to enable a VPN connection when he or she first attempts to access any HTTP URL.

If you wish to use this option, enter the desired user password once in each of the corresponding entry fields. Then set `Enable User Password` to `Yes`. (Stat on delivery: `No`).

To define one, enter the desired password twice in both entry fields.

6.9.2 Access:Language

If you select “(Automatic)” from the list of languages, the device will use the language setting of the system's browser.

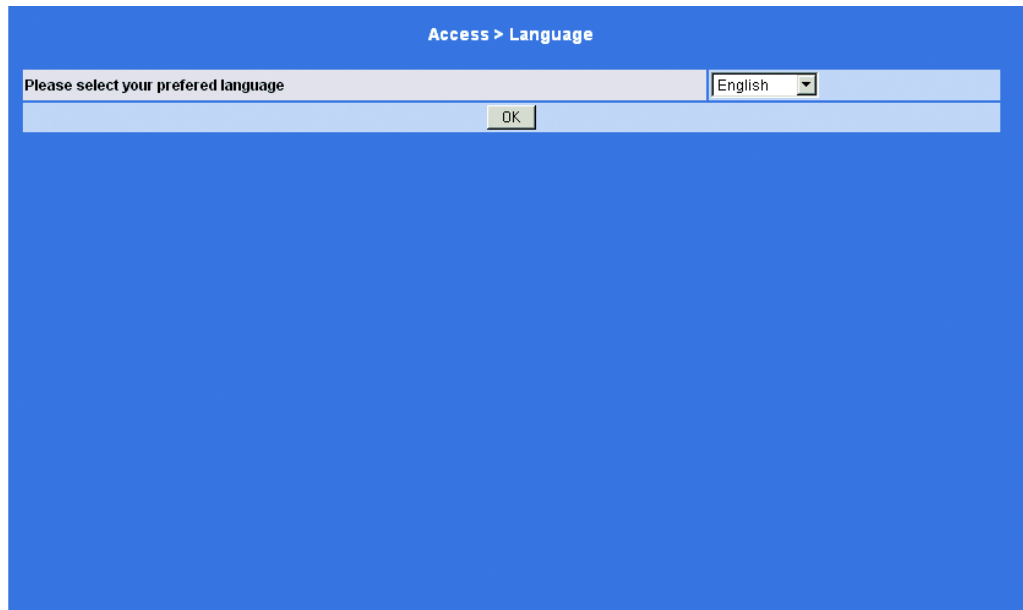
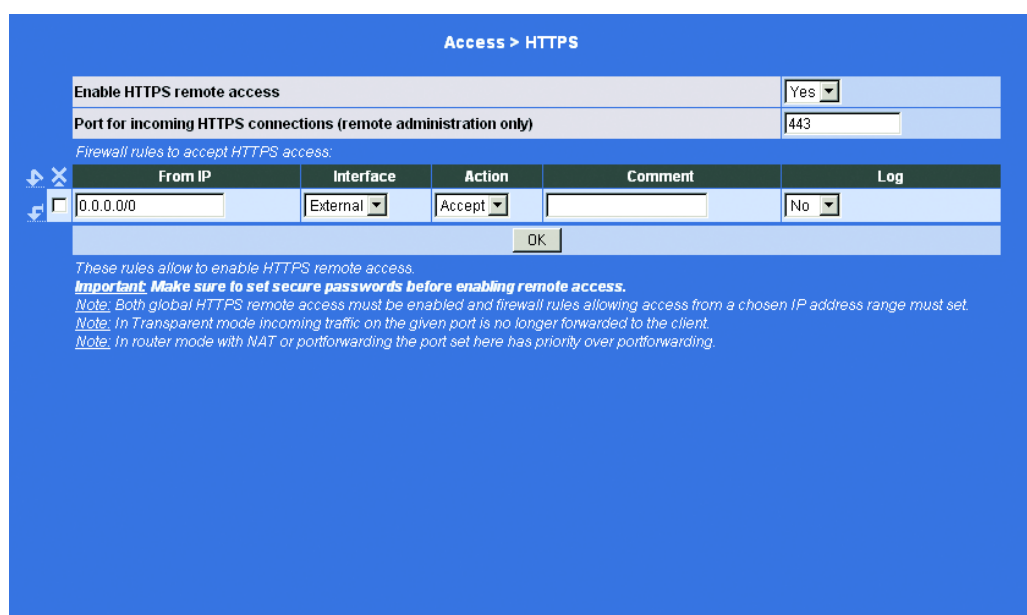


Fig. 66: *Setting the language*

6.9.3 Access:HTTPS

If HTTPS remote access is activated, the RR-EPL can be configured via its Web-based administrator interface from a computer connected to the insecure port. This means that a browser is used on the remote computer to configure the local RR-EPL.

This option is enabled by default.



Access > HTTPS

Enable HTTPS remote access Yes

Port for incoming HTTPS connections (remote administration only) 443

Firewall rules to accept HTTPS access:

	From IP	Interface	Action	Comment	Log
<input checked="" type="checkbox"/>	0.0.0.0/0	External	Accept		No

OK

These rules allow to enable HTTPS remote access.
Important: Make sure to set secure passwords before enabling remote access.
Note: Both global HTTPS remote access must be enabled and firewall rules allowing access from a chosen IP address range must set.
Note: In Transparent mode incoming traffic on the given port is no longer forwarded to the client.
Note: In router mode with NAT or portforwarding the port set here has priority over portforwarding.

Fig. 67: Access:HTTPS

IMPORTANT: If you enable remote access, make sure that a secure root and administrator password have been defined.

To prevent HTTPS remote access, make the following settings:

■ **Disable HTTPS remote access**

If you wish to prevent HTTPS, set this switch to **No**.

Note: Ensure that in this case the firewall rules on this end have been set so that it possible to access the RR-EPL from an external terminal.

■ **Port for incoming HTTPS connections (remote administration only)**

Standard: 443

You can set another port.

The remote terminal that performs the remote access must add the port number defined here to the end of the IP address when it assigns the address.

Example:

If this RR-EPL can be reached at the address 192.144.112.5 over the Internet, and if port number 443 has been set for remote access, this port number does not have to be added to the end of the address in the Web browser at the remote terminal.

When using a different port number, this number must be added to the end of the IP address, e.g.: 192.144.112.5:442.

■ **Firewall rules to accept external HTTPS access**

Lists the firewall rules that have been set up. They apply to the incoming data packets of an HTTP remote access attempt.

► Editing rule

Define the desired rule (see above) and click **OK**.

► From IP

Enter the address(s) of the computer(s) which is/are permitted remote access.

The following entry options are available:

– IP address: 0.0.0.0/0 means all addresses. To indicate a range, use the CIDR notation - see [“CIDR \(Classless InterDomain Routing\)” on page 160](#).

► Interface

external (fixed)

- **Action**
Options: `Accept` / `Reject` / `Drop`

Action	Meaning
Accept	the data packets are permitted to pass through.
Reject	the data packets are rejected, and the sender is notified that the data was rejected. In transparent mode, <code>Reject</code> has the same effect as <code>Discard</code> , see above.
Drop	the data packets are not permitted to pass through. They are “swallowed”, and the sender is not notified about what happened to the data.

Table 14: Actions for HTTPS access

Note: In Transparent mode `Reject` is supported if the local IP address is entered correctly.

- **Log**
For each individual firewall rule you can decide if, when the rule is applied,
– the event should be logged – set `Log` to `Yes`
– or not – set `Log` to `No` (factory default setting).

6.9.4 Access:SSH

If SSH remote access is activated, the RR-EPL can be configured by the computer connected to the insecure port by making an entry on the command line.
This option is enabled by default.

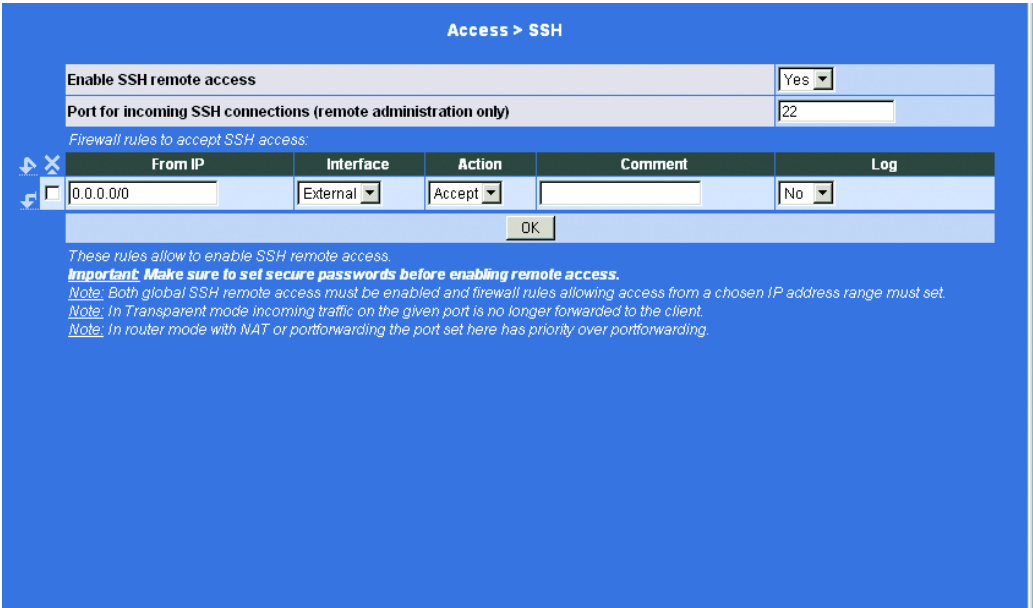


Fig. 68: Access:SSH

IMPORTANT: If you enable remote access, make sure that a secure root and administrator password have been defined.

To restrict SSH remote access, make the following settings:

■ **Disable SSH remote access**

If you wish to prevent SSH remote access, set this switch to No.

Note: Ensure that in this case the firewall rules on this end have been set so that it is possible to access the RR-EPL from an external terminal.

■ **Port for incoming SSH connections (remote administration only)**

Standard: 22

You can set another port.

The remote terminal that performs the remote access must add the port number defined here to the end of the IP address when it assigns the address.

Example:

If this RR-EPL can be reached at the address 192.144.112.5 over the Internet, and if port number 22 has been set for remote access, this port number does not have to be specified in the SSH client.

This must be specified for another port number (e.g. 22222), for example:
`ssh -p 22222 192.144.112.5`

■ **Firewall rules to accept external SSH access**

Lists the firewall rules that have been established. They apply to the incoming data packets of an SSH remote access connection.

▶ Editing rule

Define the desired rule (see above) and click OK.

▶ From IP

Enter the address(s) of the computer(s) which is/are permitted remote access.

The following entry options are available:

– IP address: 0.0.0.0/0 means all addresses. To indicate a range, use the CIDR notation - see [“CIDR \(Classless InterDomain Routing\)” on page 160](#).

▶ Interface

external (fixed)

- Action
Options: Accept / Reject / Drop

Action	Meaning
Accept	the data packets are permitted to pass through.
Reject	the data packets are rejected, and the sender is notified that the data was rejected. In transparent mode, Reject has the same effect as Discard, see above.
Drop	the data packets are not permitted to pass through. They are “swallowed”, and the sender is not notified about what happened to the data.

Table 15: Actions for HTTPS access

Note: In Transparent mode Reject is supported if the local IP address is entered correctly.

- Log
For each individual firewall rule you can decide if, when the rule is applied,
– the event should be logged – set Log to Yes
– or not – set Log to No (factory default setting).

6.9.5 Access:SNMP

SNMP (Simple Network Management Protocol) is mainly used in more complex networks to monitor the status and operation of devices. SNMP is available in several releases: SNMPv1/SNMPv2 and SNMPv3. The older versions SNMPv1/SNMPv2 do not use encryption and are not considered to be secure. We therefore recommend that you do not use SNMPv1/SNMPv2.

As far as security is concerned, SNMPv3 is considerably better, but not all management consoles support it.

Note: When you use SNMPv1, set up a VPN connection between the management station and the RR-EPL. The SNMPv1 passwords will then be transmitted invisibly.

Access > SNMP

Enable SNMPv3 access	Yes
Enable SNMPv1/v2 access	Yes
SNMPv1/SNMPv2 read-write Community String	private
SNMPv1/SNMPv2 read-only Community String	public
Port for incoming SNMP connections (external interface only)	161

Firewall rules to accept SNMP access:

From IP	Interface	Action	Comment	Log
<input type="checkbox"/> 0.0.0.0/0	External	Accept		No

These rules allow to enable SNMP access.
Important: Make sure to set secure passwords for SNMPv3 before enabling remote access.
Note: Both global SNMP access must be enabled and firewall rules allowing access from a chosen IP address range must set.
Note: In Transparent mode incoming traffic on the given port is no longer forwarded to the client.
Note: In router mode with NAT or portforwarding the port set here has priority over portforwarding.
Note: Enabling SNMP access automatically accepts incoming ICMP packets.

Fig. 69: Access:SNMP

■ **Disable SNMPv3 access**

If you wish to prevent monitoring of the RR-EPL via SNMPv3, set this switch to **No**.

Unlike SNMPv1/v2 no login data is required, since the protocol itself organises a secure authentication.

The factory setting for access via SNMPv3, requires an authentication with a login and password. These entries are:

Login: admin

Password: private

MD5 is supported for the authentication; DES is supported for encryption.

■ **Disable SNMPv1/2 access**

If you wish to prevent monitoring of the RR-EPL via SNMPv1/v2, set this switch to **No**.

In addition, you must enter the following login data:

- SNMPv1 and SNMPv2 read-write Community String
- SNMPv1 and SNMPv2 read-only Community String

Enter the required login data in these two fields.

■ **Port for incoming ANMP connections (external interface only)**

Standard: 161

■ **Firewall rules to accept external SNMP access**

Lists the firewall rules that have been set. These apply for the incoming data packets of an SNMP remote access.

► Editing rule

Define the desired rule (see above) and click **OK**.

► From IP

Enter the address(s) of the computer(s) on which SNMP monitoring is permitted.

The following options are available:

- IP address: 0.0.0.0/0 means all addresses. To indicate a range, use the CIDR notation - see [“CIDR \(Classless InterDomain Routing\)” on page 160](#).

- ▶ Interface
external (fixed)
- ▶ Action
Options: Accept / Reject / Drop

Action	Meaning
Accept	the data packets are permitted to pass through.
Reject	the data packets are rejected, and the sender is notified that the data was rejected. In transparent mode, <code>Reject</code> has the same effect as <code>Discard</code> , see above.
Drop	the data packets are not permitted to pass through. They are “swallowed”, and the sender is not notified about what happened to the data.

Table 16: Actions for HTTPS access

Note: For security reasons, the RR-EPL responds exclusively to ICMP echo requests (ping) from computers that are permitted access via SNMP.

- ▶ Log
For each individual firewall rule you can decide if, when the rule is applied,
 - the event should be logged – set Log to `Yes`
 - or not – set Log to `No` (factory default setting).

6.9.6 Access:Serial Port/Modem

This dialog allows you to configure the dial-in access via a modem.

In transparent mode (SCT/MCT) you can access the RR-EPL directly via a modem.

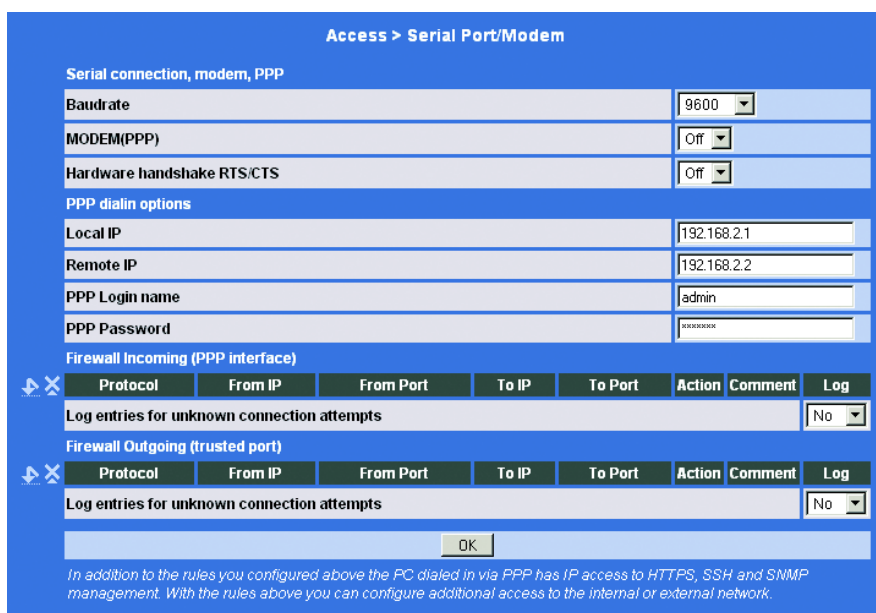
In router mode you can also access the secured network according to the firewall rules in this dialog.

Note: Use the Hirschmann modem cable to connect the modem (see [“Accessories” on page 193](#)).

The socket housing is electrically connected to the front panel of the device. The signal lines are electrically isolated from the supply voltage (60 V insulation voltage) and the front panel.

State on delivery:

- Speed:9600 Baud
- Data:8 bit
- Stopbit:1 bit
- Handshake:off
- Parity:none



Access > Serial Port/Modem

Serial connection, modem, PPP

Baudrate: 9600

MODEM(PPP): Off

Hardware handshake RTS/CTS: Off

PPP dialin options

Local IP: 192.168.2.1

Remote IP: 192.168.2.2

PPP Login name: admin

PPP Password: password

Firewall Incoming (PPP interface)

Protocol	From IP	From Port	To IP	To Port	Action	Comment	Log
Log entries for unknown connection attempts							No

Firewall Outgoing (trusted port)

Protocol	From IP	From Port	To IP	To Port	Action	Comment	Log
Log entries for unknown connection attempts							No

OK

In addition to the rules you configured above the PC dialed in via PPP has IP access to HTTPS, SSH and SNMP management. With the rules above you can configure additional access to the internal or external network.

Fig. 70: Serial Port/Modem

■ **Serial connection, modem, PPP**

- ▶ Baud rate
Select the same baud rate as the modem.

Note: A change in the baud rate has an effect on terminal operation.

- ▶ MODEM (PPP)
Enable access for the modem. An enabled modem prevents access to the terminal.
- ▶ Hardware handshake RTS/CTS
Select the same baud rate as for the modem.

■ **PPP dial-in options**

- ▶ Local IP
IP address of the RR-EPL for the serial port.
- ▶ Remote IP
IP address of the device connected to the serial port.
- ▶ PPP Login name
- ▶ PPP Password

■ **Firewall Incoming (PPP interface)**

Lists the firewall rules that have been established. They apply to the incoming data packets of a remote access connection from a modem in the direction of the secured network.

- ▶ Editing rule
Define the desired rule (see above) and click **OK**.
- ▶ From IP
Enter the address(s) of the computer(s) on which modem monitoring is permitted.
The following options are available:
 - IP address: 0.0.0.0/0 means all addresses. To indicate a range, use the CIDR notation - see [“CIDR \(Classless InterDomain Routing\)” on page 160](#).

- ▶ From port
If you wish to set a new rule, click `Arrow down`.
Define the desired rule (see above) and click `ok`.
- ▶ To IP
If you wish to set a new rule, click `arrow down`.
Define the desired rule (see above) and click `ok`.
- ▶ To port
If you wish to set a new rule, click `arrow down`.
Define the desired rule (see above) and click `OK`.
- ▶ Action
Options: `Accept / Reject / Drop`

Action	Meaning
Accept	the data packets are permitted to pass through.
Reject	the data packets are rejected, and the sender is notified that the data was rejected. In transparent mode, <code>Reject</code> has the same effect as <code>Discard</code> , see above.
Drop	the data packets are not permitted to pass through. They are “swallowed”, and the sender is not notified about what happened to the data.

Table 17: Actions for modem access

Note: In Transparent mode `Reject` is supported if the local IP address is entered correctly.

- ▶ Log
For each individual firewall rule you can decide if, when the rule is applied,
 - the event should be logged – set Log to `Yes`
 - or not – set Log to `No` (factory default setting).

■ Internal server (trusted port)

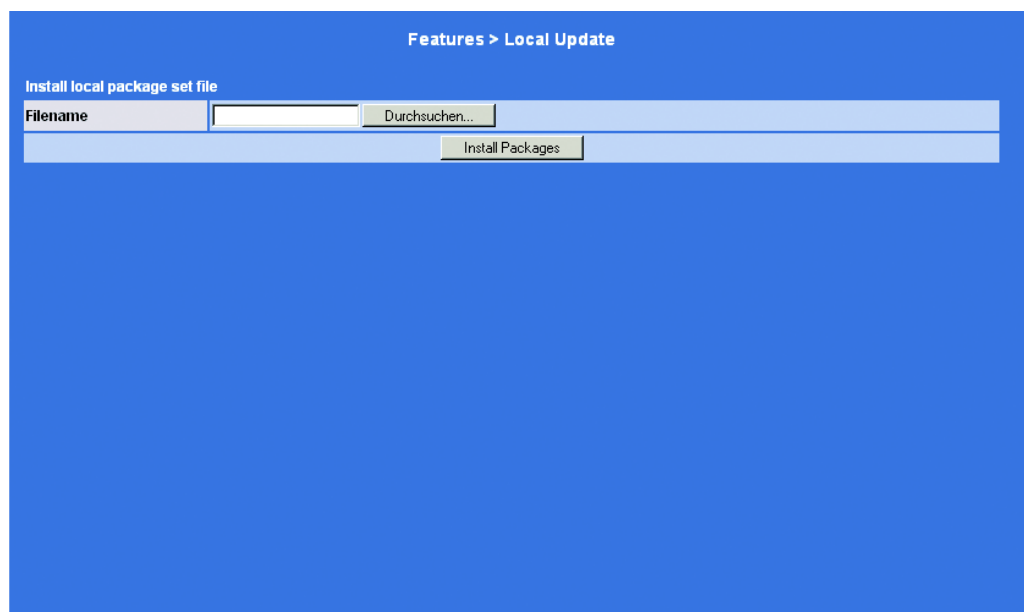
Lists the firewall rules that have been established. They apply to the outgoing data packets of a remote access connection from a modem.

6.10 Features menu

6.10.1 Features:Local Update

Prerequisite: You must have a current software package saved locally on your configuration system.

Note: For information as to whether or not and, if so, in which manner you can obtain a software update, please contact Hirschmann.



Features > Local Update

Install local package set file

Filename

Fig. 71: Local Update

If you have saved a current software update on your configuration computer, proceed as follows:

- ☐ Please read the README file!
- ☐ Click on `Browse . . .` and then select the file.

- ☐ Click installed packets to load them into the device.
This procedure can take several minutes depending on the size of the update.
If a reboot is required after the system update, this will be displayed.

6.10.2 Features:Online Update

Prerequisite: You must have a current software package available from a remote server.

Note: Ask your distributor or check the Hirschmann website to see whether, and how, you can obtain a software update.

Features > Online Update			
Install from remote repositories			
Package set name		<input type="text"/>	
		<input type="button" value="Install Package Set"/>	
Update Servers			
	Protocol	Server	Login
<input checked="" type="checkbox"/>	http://	update.eagle.hirschma	<input type="text"/>
			<input type="text"/>
<input type="button" value="OK"/>			

Fig. 72: Local Update

If you have saved a current software update on your configuration computer, proceed as follows:

- ☐ Enter the name for the “package set”. You can obtain this name from your distributor or on the Hirschmann website. The name is in the form: update-1.02-03.0.00.tar.gz
- ☐ Select the protocol you want to use for the update.
- ☐ Enter the server address under “Update Server”.
Example: update.rr-epl.hirschmann.com
- ☐ If you have selected https as the transfer protocol, then you also enter the login name and the password. The Hirschmann server uses http without password.
- ☐ Click “OK”, to load the update.
This procedure can take several minutes, depending on the size of the update. If a reboot is required after the system update, this will be displayed.

6.10.3 Features:Software Information - Display

This page lists the software modules (packages) currently loaded in the device. Each of these is called a package.

The purpose of this page is to provide the information required prior to making an update: Compare the displayed package version numbers with those of the corresponding current packages. For the relevant information, please contact your distributor.

If new versions are available, you can update the software in the device (see [“Features:Local Update” on page 151](#)).

Features > Software Information			
Version	01.0.00-pre23.eplrr		
Base	01.0.00-pre23.eplrr		
Updates	[none]		
Package Versions			
Package	Number	Version	Flavour
bootloader	0	1.2.0	default
bridge-utils	0	0.9.5	default
busybox	0	1.1.4	default
djbdns	0	1.5.0	default
eagle-hidiscovey	0	0.5.12	eplrr
ebtables	0	0.3.0	default
eplrr-mod	0	0.1.40	default
ez-ipupdate	0	3.0.12	default
fnord	0	1.9.3	default
freeswan	0	1.107.3	default
gai	0	0.19.3	default
iproute	0	1.8.24	default
iptables	0	1.5.6	default
keepalived	0	0.2.4	default
l2tpd	0	0.1.4	default
libc	0	2.4.0	default

Fig. 73: Software Information

6.10.4 Features:Hardware information

Only for experienced system administrators or Support.

Features > Hardware Information	
Hardware	Hirschmann Eagle TX/TX
CPU	XScale-IXP4xx/IXC11x rev 1 (v5b)
CPU Family	IXP4XX
CPU Stepping	B0
CPU Clock Speed	533 MHz
System Temperature	40.0°C
System Uptime	22:41
User Space Memory	63220 kB
MAC 1	00:80:63:06:8f:27
MAC 2	00:80:63:06:8f:28
MAC 3	00:80:63:06:8f:29
Serial Number	943011001010201357
Version Parameterset	3

Fig. 74: Hardware information

6.11 Support menu

6.11.1 Support:Snapshot

This function creates a compressed file (in the tar format), which contains all current configuration settings and log entries, that are relevant for error diagnostics. This file does not contain any private information such as the private machine certificate or passwords. However, any pre-shared keys used for VPN connections are included in the snapshots. If requested, please provide this file to Hirschmann-Support.

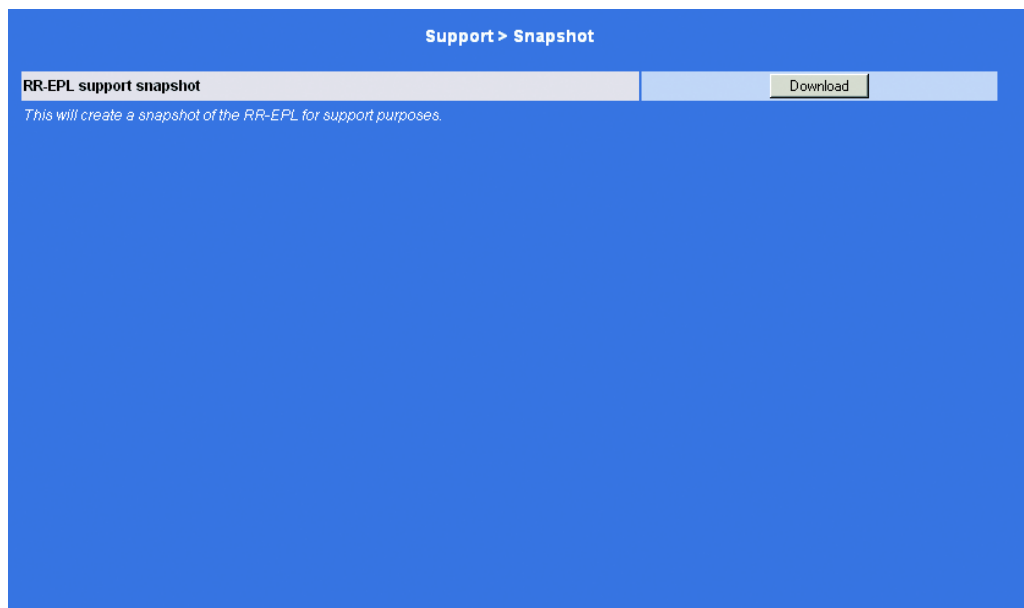


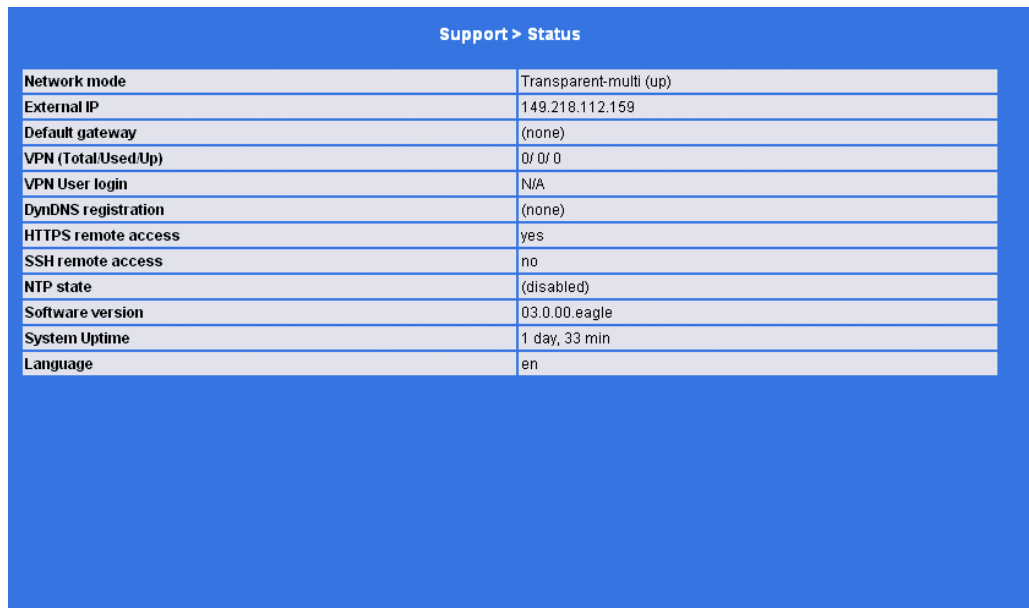
Fig. 75: Snapshot

To create a snapshot, proceed as follows:

- ☐ Click Download.
- ☐ Save the file under the name `snapshot.tar.gz`
- ☐ Please make the file available to Hirschmann Support, if so requested.

6.11.2 Support:Status - Display

Displays a summary of various status information for support purposes:



Network mode	Transparent-multi (up)
External IP	149.218.112.159
Default gateway	(none)
VPN (Total/Used/Up)	0/ 0/ 0
VPN User login	N/A
DynDNS registration	(none)
HTTPS remote access	yes
SSH remote access	no
NTP state	(disabled)
Software version	03.0.00.eagle
System Uptime	1 day, 33 min
Language	en

Fig. 76: Support:Status

■ Network mode

The RR-EPL's mode of operation

- ▶ Transparent (SCT/MCT)
- ▶ Router
- ▶ PPPoE
- ▶ PPTP

■ Externe IP

The IP address of the RR-EPL at its connection for the network (WAN or Internet) connected to the insecure port.

In transport mode, the RR-EPL takes on the local IP address.

■ **Default gateway**

The default gateway address is shown here that is entered in the RR-EPL.

■ **VPN**

Supports:

- ▶ Total: Total number of VPN connections setup
- ▶ Used: Number of VPN connections used
- ▶ Up: Number of VPN connections currently active

■ **DynDNS registration**

Supports:

- ▶ none: no DynDNS server specified
- ▶ DynDNS Server: Address of the DynDNS server, at which the RR-EPL should register.
- ▶ failure: The RR-EPL has unsuccessfully attempted to setup a connection to the DynDNS server.
- ▶ trying: The RR-EPL is currently attempting to setup a connection to the DynDNS server.

■ **HTTPS remote access**

Possible settings

- ▶ no
- ▶ yes

■ **SSH remote access**

Possible settings

- ▶ no
- ▶ yes

■ NTP Status

Options:

- ▶ `synchronized`: The RR-EPL receives the current time from a time server (Greenwich time) via the Network Time Protocol.
- ▶ `not synchronized`: The RR-EPL is not connected to a time server and can thus not provide the current time.

■ Software version

Shows the version of the software installed in the RR-EPL

■ System Uptime

This shows how much time has elapsed since the last time that the RR-EPL was started.

■ Language

This field shows the currently selected language.

6.12 CIDR (Classless InterDomain Routing)

IP netmasks and CIDR are notations, which define an address space containing multiple IP addresses. In this case, an address space in which the addresses follow one another sequentially is treated as a network. CIDR reduced the e.g. routing tables stored in routers to a network postfix in the IP address. With this postfix, an aggregate of many networks can be identified. The method is described in RFC 1518.

To define a range of IP addresses for the RR-EPL e.g. when configuring the firewall, it may be necessary to use the CIDR notation to specify the address space. The following table presents the IP netmask on the left and the corresponding CIDR notation on the right.

IP binary CIDR

```

255.255.255.25511111111 11111111 11111111 11111111 32
255.255.255.25411111111 11111111 11111111 11111110 31
255.255.255.25211111111 11111111 11111111 11111100 30
255.255.255.24811111111 11111111 11111111 11111000 29
255.255.255.24011111111 11111111 11111111 11110000 28
255.255.255.22411111111 11111111 11111111 11100000 27
255.255.255.19211111111 11111111 11111111 11000000 26
255.255.255.12811111111 11111111 11111111 10000000 25

```

```

255.255.255.0111111111 11111111 11111111 00000000 24
255.255.254.0111111111 11111111 11111110 00000000 23
255.255.252.0111111111 11111111 11111100 00000000 22
255.255.248.0111111111 11111111 11111000 00000000 21
255.255.240.0111111111 11111111 11110000 00000000 20
255.255.224.0111111111 11111111 11100000 00000000 19
255.255.192.0111111111 11111111 11000000 00000000 18
255.255.128.0111111111 11111111 10000000 00000000 17

```

```

255.255.0.0111111111 11111111 00000000 00000000 16
255.254.0.0111111111 11111110 00000000 00000000 15
255.252.0.0111111111 11111100 00000000 00000000 14
255.248.0.0111111111 11111000 00000000 00000000 13
255.240.0.0111111111 11110000 00000000 00000000 12
255.224.0.0111111111 11100000 00000000 00000000 11
255.192.0.0111111111 11000000 00000000 00000000 10
255.128.0.0111111111 10000000 00000000 00000000 9

```

```

255.0.0.0111111111 00000000 00000000 00000000 8
254.0.0.0111111110 00000000 00000000 00000000 7
252.0.0.0111111100 00000000 00000000 00000000 6
248.0.0.011111000 00000000 00000000 00000000 5
240.0.0.011110000 00000000 00000000 00000000 4
224.0.0.011100000 00000000 00000000 00000000 3
192.0.0.011000000 00000000 00000000 00000000 2
128.0.0.010000000 00000000 00000000 00000000 1

```

```

0.0.0.000000000 00000000 00000000 00000000 0

```

Example: 192.168.1.0 / 255.255.255.0 corresponds to 192.168.1.0/24 in CIDR notation.

6.13 Example of a network

The diagram below illustrates how in a local network with subnetworks the IP address could be distributed, what the resulting network addresses would be, and how an additional internal router would be specified.

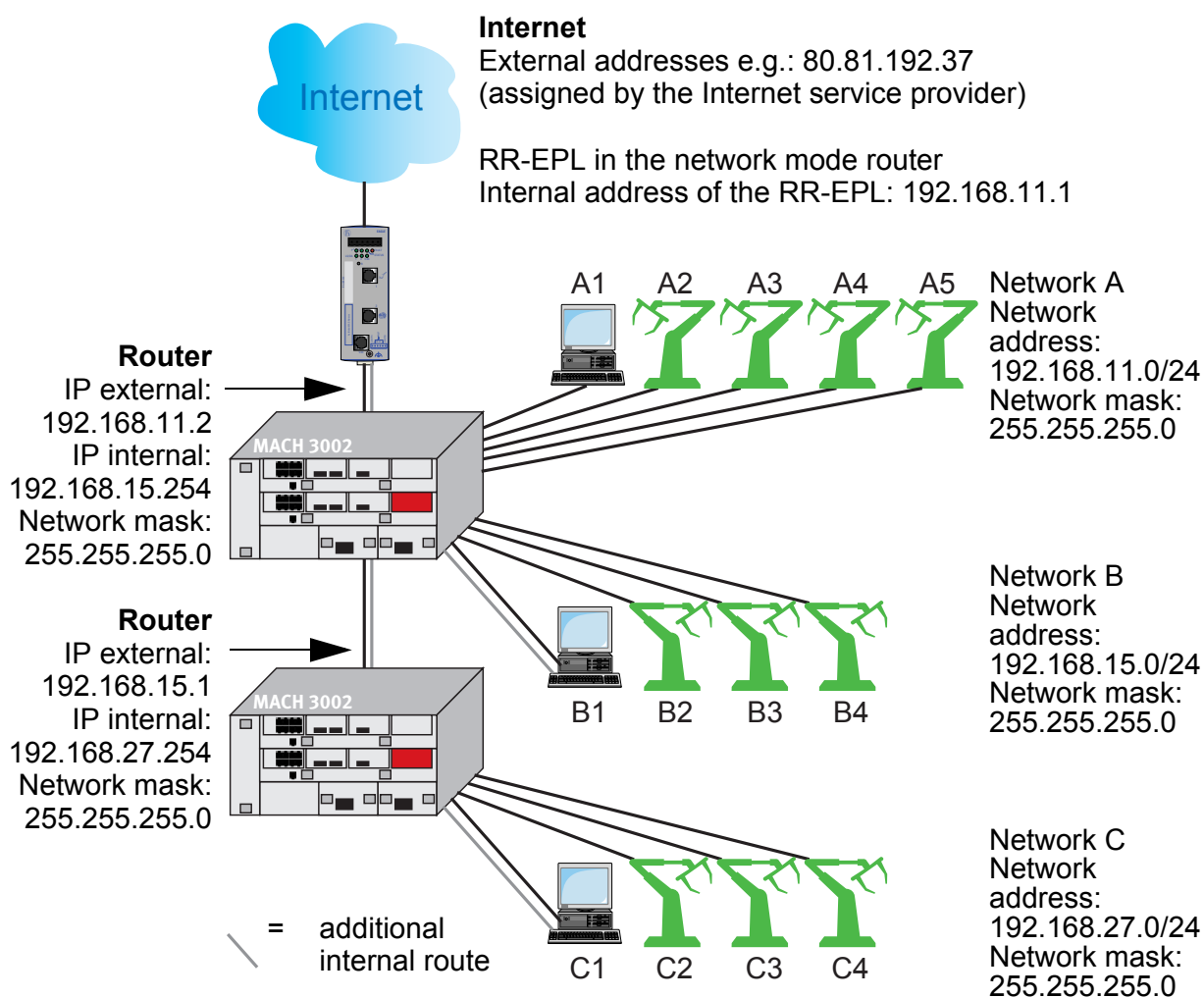


Fig. 77: Network example

Computer	A1	A2	A3	A4	A5
IP address	192.168.11.3	192.168.11.4	192.168.11.5	192.168.11.6	192.168.11.7
Network mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Table 18: Network A

Computer	B1	B2	B3	B4
IP address	192.168.15.2	192.168.15.3	192.168.15.4	192.168.15.5
Network mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Table 19: Network B

Computer	C1	C2	C3	C4
IP address	192.168.27.1	192.168.27.2	192.168.27.3	192.168.27.4
Network mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Table 20: Network C

Network	Gateway
192.168.15.0/24	192.168.11.2
192.168.27.0/24	192.168.11.2

Table 21: Additional internal routes for RR-EPL (see “[Network:Base](#)” on page 72)

7 The Recovery button

The Recovery button enables you to,

- ▶ perform a restart,
- ▶ perform the Recovery procedure and
- ▶ to flash the firmware.

7.1 Performing a restart

The RR-EPL offers several ways of performing a restart.

- ▶ Restart with Recovery button
 - ☐ To perform a restart, press the Recovery button longer than 1.5 seconds and less than 7 seconds until the STATUS LED goes out and the FAULT LED lights up red.
- ▶ The supply of current is temporarily interrupted.
- ▶ Management Web interface
See [“System:Reboot” on page 59](#).
- ▶ Management SNMP
with the MIB object `hmSecAction`.

7.2 Executing the recovery procedure

7.2.1 Aim

The recovery procedure sets all the parameters to the state on delivery, with the exception of the passwords.

Possible reasons for executing the recovery procedure:

- ▶ The RR-EPL is in router or PPPoE mode,
- ▶ The device address of the RR-EPL has been configured differently than the default setting.
- ▶ You do not know the current IP address of the device,
- ▶ You have no way of making this setting from a V.24 terminal.

7.2.2 Action

- ☐ Perform a restart - see [“Performing a restart” on page 166](#).
- ☐ Wait until the STATUS-LED is continuously green-lit. This lasts about 30 seconds.
- ☐ Press the Recovery button slowly 6 times.
Result:
The RR-EPL responds after about 2 seconds:
The STATUS LED blinks 6 times yellow and then green.
- ☐ Press the Recovery button 6 times again within the next 60 seconds.
Result:
The device performs a restart and is reset to the state on delivery, with the exception of the passwords.

7.3 Flashing the firmware

Aim

The entire RR-EPL software is to be loaded into the device.

Note: All configured settings will be deleted. The RR-EPL is reset to its default values (state on delivery).

Possible reasons to flash the firmware:

- ▶ You have lost or forgotten the administrator password.
- ▶ The firewall rules have been set in such a way that the administrator no longer has access.

Action

Prerequisites:

- ▶ You have copied the software of the RR-EPL from the RR-EPL CD or obtained it from Hirschmann support and have saved it on the configurations computer.
- ▶ The DHCP and tftp server are installed on the same computer (see [“Requirements for flashing the firmware” on page 170](#)).

Proceed as follows:

- ☐ Keep the Recovery button pressed until the recovery status starts as follows:
The RR-EPL is restarted (after 1.5 seconds). After approx. 7 seconds the RR-EPL switches to recovery status.
Status display of the recovery status: All ports and STATUS LEDs are green-lit.
- ☐ Release the Recovery switch no more than 1 second after the device has entered its recovery state.

Note: If you do not release the Recovery quickly enough, the RR-EPL will restart again.

Result:

The RR-EPL starts the recovery system. It searches for the DHCP server via the computer connected to the secure port or via the connected network in order to obtain an IP address from it.

- ▶ **Status display:** The STATUS LED blinks.
The file `install.p7s` is loaded from the tftp server. It contains the electronically signed control procedure for the installation procedure. Only files that have been signed by Hirschmann are loaded.
The control procedure then deletes the flash memory and prepares the reinstallation of the software.
 - ▶ **Status display:** Die 3 port LEDs form a sequential light.
The software `jffs2.img.p7s` is then downloaded from the tftp server and stored in the flash memory. This file contains the actual RR-EPL-operating system and is electronically signed. Only files that have been signed by Hirschmann are accepted.
 - ▶ **Status display:** Die 3 port LEDs form a sequential light.
It takes about 3 to 5 minutes to delete and store the file.
The RR-EPL is then restarted automatically.
The new software is then unpacked and configured.
This takes about 5 minutes.
 - ▶ **Status display:** The STATUS LED blinks.
Once the procedure has ended, all port LEDs blink green simultaneously.
- ☐ **Restart the RR-EPL.**
To do this, press the Recovery button until the STATUS LED goes out.
or
Disconnect the device from power supply and then reconnect it.

Result:

The RR-EPL is in the delivery state. Reconfigure it (see [“Setting up a local configuration connection” on page 42](#)).

7.3.1 Requirements for flashing the firmware

To flash the firmware, a DHCP and tftp server must be installed on the locally connected computer or network computer.

(DHCP = Dynamic Host Configuration Protocol; tftp = Trivial File Transfer Protocol)

- ☐ Install the DHCP and tftp server, if needed (see below).

Note: If you install a second DHCP server in a network, this can affect the configuration of the entire network!

7.3.2 Installing the DHCP and tftp server under Windows

Install the software for the tftp server and DHCP server, that is located on the CD. Proceed by following the steps below:

- ☐ If the Windows system is connected to network, disconnect it.
- ☐ Copy the software into any empty folder on the Windows system.
Start the program `TFTPD32.EXE`.
The image files are also found on the CD-ROM, which was included in the package.

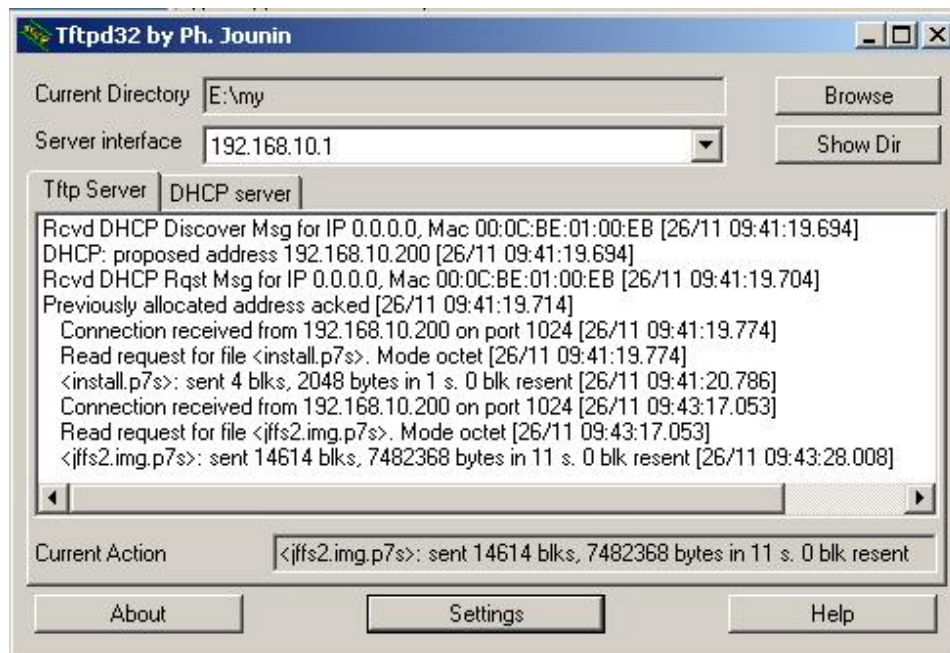


Fig. 78: Start screen of the TFTPD32 program

- ☐ The server IP must be set to: 192.168.10.1
This must also be the address of the network adapter.
Click on the Browse button to switch to the folder in which the RR-EPL image files have been saved: `install.p7s`, `jffs2.img.p7s`

- Click on the `tftp` Server or DHCP Server tab and then click on the Settings button to open the dialog shown below. Then set the parameters as shown:

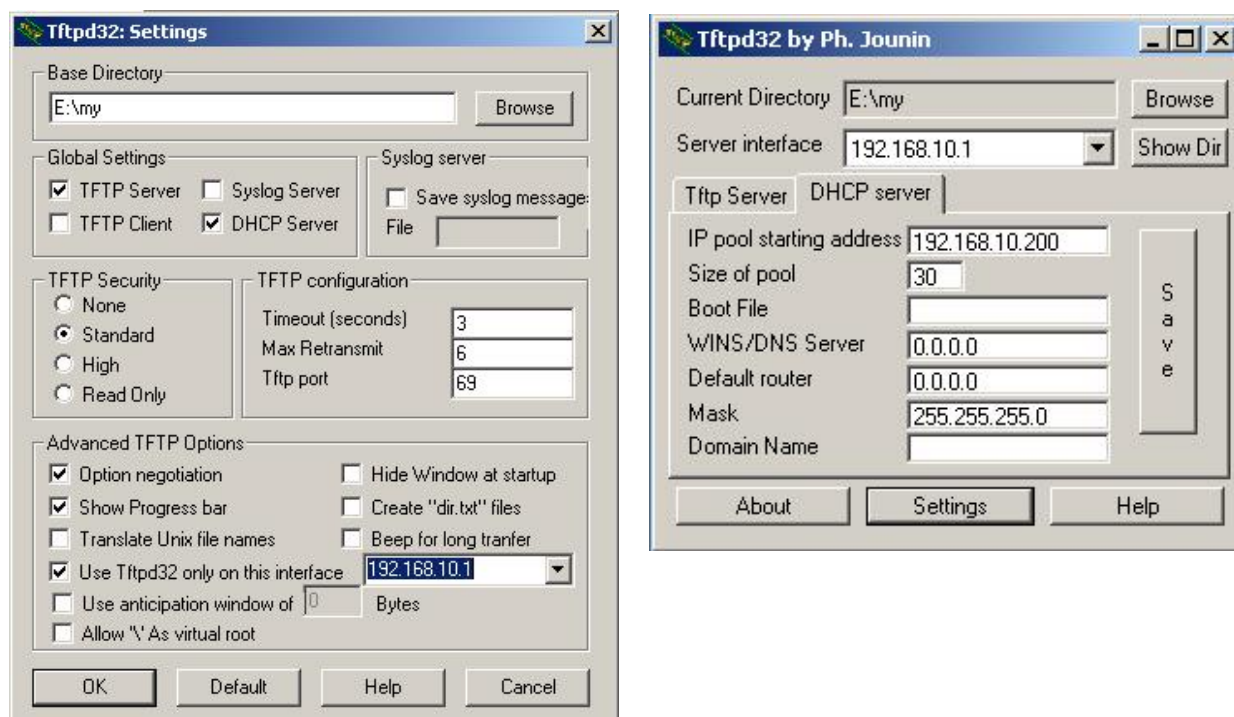


Fig. 79: Settings

7.3.3 Installing DHCP and TFTP servers under Linux

All current Linux distributions include DHCP and TFTP servers. Install the corresponding packages in accord with the instructions for the respective distribution.

- ☐ Configure the DHCP server by making the following settings in the `/etc/dhcp` file:

```
subnet 192.168.134.0 netmask 255.255.255.0 {  
  range 192.168.134.100 192.168.134.119;  
  option routers 192.168.134.1;  
  option subnet-mask 255.255.255.0;  
  option broadcast-address 192.168.134.255;}
```

This sample configuration makes 20 IP addresses (.100 to .119) available. It is assumed that the DHCP server has the address 192.168.134.1 (settings for ISC DHCP 2.0).

The required TFTP server is configured in the following file:
`/etc/inetd.conf`

- ☐ In this file, insert the appropriate lines or set the necessary parameter for the TFTP service (the directory for data is: `/tftpboot`)

```
tftp dgram udp wait root /usr/sbin/in.tftpd -s /tftpboot/
```

- ☐ Then restart the `inetd` process to activate the modified configuration. If you use a different mechanism, e.g. `xinetd`, please read the corresponding documentation.

8 HiConfig

HiConfig is a command-line oriented program for configuring the RR-EPL. The HiConfig interface can be reached via

- ▶ the secure port,
- ▶ the insecure port or
- ▶ the V.24 port.

■ Making a connection the HiConfig over a LAN

PuTTY is a terminal program with which you can establish a secure connection to the HiConfig interface of the RR-EPL from your PC over the LAN.

- ☐ Copy the putty.exe file from the enclosed CD to your PC's hard disk.
- ☐ Start PuTTY by doubleclicking this file.

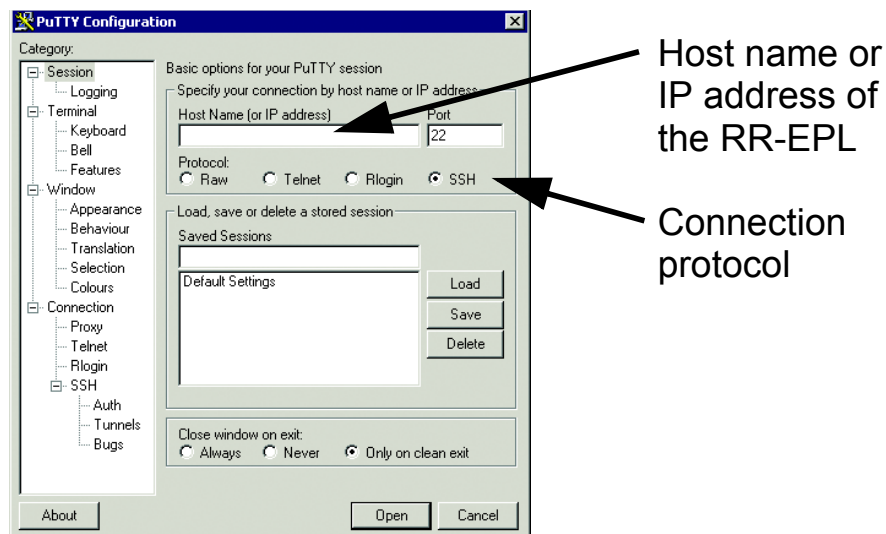


Fig. 80: Connection setup

- ☐ Enter the host name or the IP address of the RR-EPL.
- ☐ Select the connection protocol.
 - SSH, if your PC accesses the RR-EPL from within a LAN.

- ☐ Click Open.
PuTTY establishes a connection to the RR-EPL and opens the login window.
- ☐ Press the Enter key.
The RR-EPL operating system will prompt you to enter the username (admin or root).
- ☐ Enter the username.
The RR-EPL operating system will prompt you to enter the password (private or root).
- ☐ Enter the password.
The RR-EPL operating system responds with the “\$” prompt (for admin) or “#” (for root).
- ☐ Enter `hiconfig` (please note that entries are case-sensitive) and press the Enter key.
HiConfig responds by displaying a list of valid commands.

```
delete the current row
--delete-all-rows
delete all rows
--silent
DON'T reconfigure services
(the gaidd session daemon isn't required when option is used)

--get-all
dump all configuration data to stdout
--set-all
read all configuration data from stdin

--cache <file>
alternative location for the cache file
--socket <file>
use an alternative unix domain socket

Examples:
hiconfig --set ROUTERMODE router
hiconfig --set VPN.1.GATEWAY 192.168.1.1
hiconfig --goto VPN.0 --set .GATEWAY %any --set .ENABLED no
hiconfig --goto VPN --add-row --set .NAME tokyo --set .GATEWAY
146.215.5.34
hiconfig --goto VPN.2 --delete-row
#
```

Fig. 81: HiConfig start page

■ Making a connection to HiConfig over a V.24 port.

The V.24 port allows you to configure the RR-EPL, in the event access via the LAN ports is not possible. The cause for this can be: failed autonegotiations, faulty firewall configuration, etc.

- ☐ Using the terminal cable, connect your PC to the V.24 port of the RR-EPL.

Example of establishing a terminal connection under Windows 2000:

- ☐ Choose:

Start:Programs:Accessories:Communication:
HyperTerminal

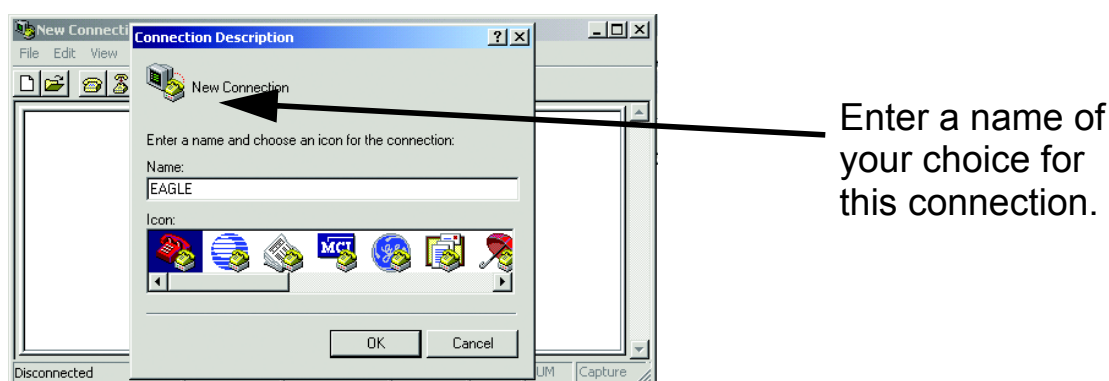


Fig. 82: Setting up the terminal connection

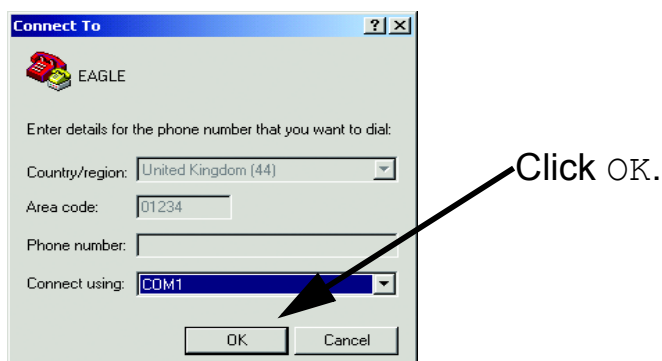
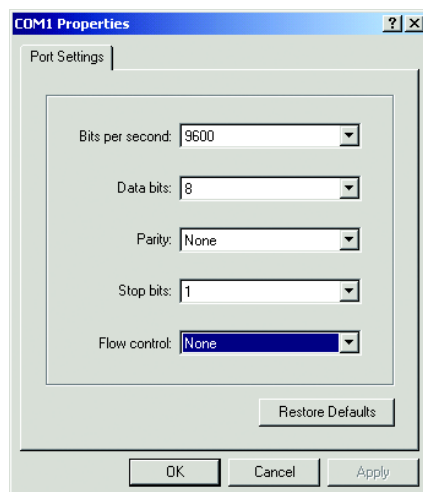


Fig. 83: Terminal connection without phone number



Enter the connection settings and click OK.

Fig. 84: Properties of the terminal connection

- ☐ Press the Enter key.
The RR-EPL operating system will prompt you to enter the username (admin or root).
- ☐ Enter the username.
The RR-EPL operating system will prompt you to enter the password (private or root).
- ☐ Enter the password.
The RR-EPL operating system responds with the "\$" prompt (for admin) or "#" (for root).
- ☐ Enter `hiconfig` (please note that entries are case-sensitive) and press the Enter key.
HiConfig responds by displaying a list of valid commands.

```
    delete the current row
--delete-all-rows
    delete all rows
--silent
    DON'T reconfigure services
    (the gaid session daemon isn't required when option is used)

--get-all
    dump all configuration data to stdout
--set-all
    read all configuration data from stdin

--cache <file>
    alternative location for the cache file
--socket <file>
    use an alternative unix domain socket

Examples:
    hiconfig --set ROUTERMODE router
    hiconfig --set VPN.1.GATEWAY 192.168.1.1
    hiconfig --goto VPN.0 --set .GATEWAY %any --set .ENABLED no
    hiconfig --goto VPN --add-row --set .NAME tokyo --set .GATEWAY
146.215.5.34
    hiconfig --goto VPN.2 --delete-row
#
```

Fig. 85: *HiConfig start page*

■ Port Configuration

To set the port configuration you will need the following parameters:

Designation	Value
EPL port	ETH1
Insecure port	ETH0
Enable port	ENABLE
Disable port	DISABLE
Autonegotiation on	AUTONEG yes
Autonegotiation off	AUTONEG no
10 Mbit/s, halfduplex	FIXEDSETTING 10hd
10 Mbit/s, fullduplex	FIXEDSETTING 10fd
100 Mbit/s, halfduplex	FIXEDSETTING 100hd
100 Mbit/s, fullduplex	FIXEDSETTING 100fd

Table 22: Port configuration parameters

The command `hiconfig --set` and the proper parameters allow you to configure the ports.

The command `hiconfig --get-all | more` displays all the configured parameters one page at a time.

Example:

Set the secure port to 10 Mbit/s halfduplex:

```
hiconfig --set ENABLE_ETH1_AUTONEG no
hiconfig --set ETH1_FIXEDSETTING 10hd
```

Set the secure port to Autonegotiation on:

```
hiconfig -- set ENABLE_ETH1_AUTONEG yes
```


■ **IP parameter configuration in transparent mode**

- ☐ Disable DHCP-Client protocol:

```
$ hiconfig --set MGUARD_ROUTER_DHCP no
```

- ☐ IP address of the untrusted port:

```
$ hiconfig --set MY_ROUTER_IP 149.218.112.55
```

- ☐ Networkmask of the untrusted port:

```
$ hiconfig --set MY_ROUTER_NET 255.255.255.0
```

- ☐ Enter the gateway address as follows:

```
$ hiconfig --set DEFAULT_GW 148.218.112.199
```

The IP addresses and the network mask refer to the entries in the HiDiscovery example ([see Fig. 16](#)).

A Appendix

FAQ

Answers to frequently asked questions can be found at the product page of the Hirschmann Web site:

www.hirschmann.com

For detailed information on all services offered by the Hirschmann Competence Center, please visit the Web site <http://www.hicomcenter.com/>.

Based specifications and standards

■ List of norms and standards:

- ▶ EN 61000-6-2:2001 Basic standard - interference resistance in industry
- ▶ EN 55022:1998 + A1 2000 + A2 2003 - Interference characteristics for IT systems
- ▶ EN 60950:2001 - Security in IT systems
- ▶ EN 61131-2:2003 - Programmable Logic Controllers
- ▶ FCC 47 CFR Part 15:2003 – Code of Federal Regulations
- ▶ Germanischer Lloyd, Rules for Classification and Construction VI - 7 - 3 Part 1, Ed. 2003.
- ▶ cUL 508:1998 – Safety for Industrial Control Equipment
- ▶ cUL 1604 Electrical Equipment for Use in Class I and Class II, Div.2 and Class III Hazardous (Classified) Locations
- ▶ cUL 60950 Safety for Information Technology Equipment.

Certified devices are marked with a certification identifier.

■ IEEE standards

IEEE 802.1 D	Switching, GARP, GMRP, Spanning Tree
IEEE 802.1 Q	Tagging
IEEE 802.3	Ethernet

■ **Supported MIBs**

Private MIBs:

- ▶ hmprivate
- ▶ hmSecurityGateway-MIB

Standard MIBs:

- ▶ IF-MIB
- ▶ MAU-MIB
- ▶ RFC1155-SMI
- ▶ RFC1213-MIB
- ▶ SNMPv2-MIB
- ▶ SNMPv2-SMI
- ▶ SNMPv2-TC

The private MIBs are located on the enclosed RR-EPL CD-ROM.

SNMP traps

■ Private MIB:

hmSecHTTPSLoginTrap

is sent, if a login attempt was made via HTTPS.

hmSecShellLoginTrap

is sent if a login was made via the security shell or the V.24 terminal.

hmSecDHCPNewClientTrap

is sent if the DHCP server receives a request from an unknown client.

hmTemperatureTrap

is sent if the temperature exceeds / falls below the set threshold values.

hmPowerSupply

is sent if the status of the voltage supply changes.

hmSignallingRelay

is sent if the status of the signal contact changes.

hmAutoconfigAdapterTrap

is sent if the AutoConfiguration adapter ACA 11 is removed or plugged in again.

■ Standard traps:

coldStart

is sent during the boot process after successful management initialization following a cold or warm start.

linkUp

is sent if the link to a port is re-established.

linkDown

is sent if the link to a port is interrupted.

authenticationFailure

is sent if a station attempts to access an agent without permission.

Certifications

The following table lists the certification status of the RR-EPL product family.
Certified devices are marked with a certification identifier.

Standard	RR-EPL
EN 61131-2	In preparation
CE	In preparation
FCC 47 CFR Part 15	In preparation
cUL 508 / CSA C22.2 No.142	In preparation
cUL 1604 / CSA C22.2 No.213	In preparation
Germanischer Lloyd	fulfilled

Table 23: Certifications, for the current status, visit www.hirschmann.com

Technical data

RR-EPL

Dimensions W x H x D

46 x 131 x 111 mm
1.8 in x 5.2 in x 4.4 in

Weight

340 g, 0.75 lb

Top-hat rail fastener

in line with IEC 60715:1981 + A1:1995

Power supply

Operating voltage

24 V DC, -25 % +33 %
Nec Class 2 power source,
safety extra-low voltage (SELV/PELV)
redundant inputs uncoupled

Power consumption

with 2 TX ports

7.2 W maximum at 24 V DC
24.6 BTU/h

with 1 TX port and 1 FX port

8.4 W maximum at 24 V DC
28.7 BTU/h

with 2 FX ports

9.6 W maximum at 24 V DC
32.8 BTU/h

Overload current protection at input

non-changeable thermal fuse

Environment

Ambient temperature

Surrounding air:
0 °C to 60 °C (32 °F to 140 °F)

Storage temperature

Surrounding air:
-20 °C to +70 °C (-4 °F to 158 °F)

Air humidity

10 % to 95 % (non-condensing)

Atmospheric pressure

Suitable for operation at up to
2000 m (6561 ft), 795 hPa

Pollution Degree

2

Protection classes

Laser protection

Class 1 conforming to EN 60825-1
(2001)

Protection class

IP 20

EMC interference immunity

EN 61000-4-2

electrostatic discharge

contact discharge:

test level 3 (6 kV)

air discharge:

test level 3 (8 kV)

EN 61000-4-3

electromagnetic field

test level 3

(10 V/m; 80 - 2000 MHz)

EN 61000-4-4

fast transients (burst)

test level 3

(2 kV power line, 1 kV data line)

EN 61000-4-5

surge voltage

power line

symmetric: test level 2 (1kV)

asymmetric: test level 3 (2kV);

data Line: test level 2 (1kV)

EN 61000-4-6

cable-based RF faults: test level 3

10 V (150 kHz - 80 MHz)

EMC emitted immunity

EN 55022

Class A

FCC 47 CFR Part 15

Class A

Germanischer Lloyd

Rules for Classification and

Construction VI - 7 - 3 Part 1, Ed. 2003

Stability

Vibration

IEC 60068-2-6 Test FC, testing level

in line with IEC 61131-2 E2 CDV and

Germanischer Lloyd Guidelines for

the Performance of Type Tests Part 1

Shock

IEC 60068-2-27 Test Ea, testing level

in line with IEC 61131-2 E2 CDV

Interfaces

Signal contact	1 A maximum, 24 V
V.24 port	external management, modem
2 type depending ports	TX ports with RJ-45 socket, FX ports with DSC socket

Network size TX port 10BASE-T/100BASE-TX/1000BASE-TX

Length of a TP segment	100 m (328 ft) max.
------------------------	---------------------

Network size F/O ports 100BASE-FX

System attenuation	
50/125 µm fiber, multimode	0-8 dB
62.5/125 µm fiber, multimode	0-11 dB

Example for F/O line length

50/125 µm fiber, multimode	5 km/16,400 ft max. data of fiber: 1 dB/km, 800 MHz*km
62,5/125 fiber, multimode	4 km/13,120 ft max. 1 dB/km, 500 MHz*km

Scope of delivery

RR-EPL Firewall/VPN System incl.	terminal block for power supply RR-EPL manual on CDROM Description and operating instructions
----------------------------------	---

Order number

RR-EPL TX/TX	943 011-021
RR-EPL TX/MM SC	943 011-022

Accessories

Manual: "Basics of Industrial ETHERNET and TCP/IP"	280720-834
ACA Auto Configuration Adapter	943 751-001
Terminal cable	943 301-001
6-pin terminal block (50 pieces)	943 845-002
Rail Power Supply RPS 30	943 662-003
Rail Power Supply RPS 60	943 662-001
Rail Power Supply RPS 120	943 662-011
Network Management Software HiVision	943 471-100

Copyright of integrated software

The RR-EPL incorporates certain free and open software. The license terms associated with this software require that we give copyright and license information. These informations can be found on the enclosed CD-ROM.

For free software under the terms of the GPL/LGPL we also provide source code according to Subsection 3b of the GPL or Subsection 6b of the LGPL, respectively.

Please contact your Hirschmann contract partner.

B Glossar

► 3DES / DES

This symmetrical encryption algorithm was developed by IBM and checked by the NSA. DES ([“Symmetrical encryption” on page 201](#)) was set in 1977 by the American National Bureau of Standards, which was the predecessor of the National Institute of Standards and Technology (NIST), as the standard for American governmental institutions. Since this was the very first standardized encryption algorithm, it quickly won acceptance by industry even outside of America.

DES uses a 56 bit long key, which is no longer considered secure as the processing power available has greatly increased since 1977.

3DES is a variant of DES. It uses keys that are three times as long, i.e. 168 bits long. 3DES is still considered to be secure and is also included in the IPsec standard

► Asymmetrical encryption

In the case of asymmetrical encryption, data is encrypted with one key and decrypted with a second key. Either key may be used for encryption or decryption. One of the keys is kept secret by its owner (Private Key), the other is made available to the public (Public Key), i.e. possible communication partners.

A message encrypted with the public key can only be decrypted and read by the receiver who has the associated private key. A message encrypted with the private key can only be decrypted and read by a receiver who has the associated public key. The fact that the message was encrypted with the private key proves that the owner of the associated public key actually sent the message. Therefore, the expression "digital signature" is also often used.

However, asymmetrical encryption techniques such as RSA are both slow and susceptible to certain types of attack and are therefore frequently combined with some form of symmetrical encryption ([“Symmetrical encryption” on page 201](#)). On the other hand, there are concepts which avoid the additional work of administering symmetrical keys.

► AES

Advanced Encryption Standard. This encryption standard was developed by NIST (National Institute of Standards and Technology) in cooperation with the industry. This [“Symmetrical encryption” on page 201](#) was developed to replace the earlier DES standard. AES specifies three different key sizes (128, 192 and 256 bits).

In 1997, NIST started the AES initiative and announced its conditions for the algorithm. From the many proposed encryption algorithms, NIST selected a total of five algorithms for closer examination - the MARS, RC6, Rijndael, Serpent and Twofish algorithms. In October 2000, the Rijndael algorithm was adopted as the standard's encryption algorithm.

► **Certificate (X.509)**

A type of "Seal", which certifies the authenticity of a public key (["Asymmetrical encryption" on page 195](#)) and the associated data.

To enable the user of the public key, which will be used to encrypt the data, to be sure that the public key that he/she has received is really from its issuer and thus from the instance, which should later receive the data, it is possible to use certification. A Certification Authority – CA certifies the authenticity of the public key and the associated link between the identity of the issuer and his/her key. The certification authority will verify authenticity in accordance with its rules, which may, for example, require that the issuer of the public key appear before it in person. Once authenticity has been successfully certified, the certification authority will add its digital signature to the issuer's public key. The result is a Certificate.

An X.509(v3) Certificate thus includes a public key, information about the key owner (given as its Distinguished Name (DN)), the authorized usage etc. and the signature of the certification authority.

The signature is created as follows: The certification authority creates an individual bit sequence, which is known as the HASH value, from the bit sequence of the public key, the information about its owner and other data. This sequence may be up to 160 bits long. The certification authority encrypts this with its own private key and then adds it to the certificate.

The encryption with the certification authority's private key proves the authenticity of the certificate, i.e. the encrypted HASH string is the certification authority's digital signature. If the certificate's data is altered, this HASH value will no longer be correct with the consequence that the certificate will be worthless.

The HASH value is also known as the fingerprint. Since it is encrypted with the certification authority's private key, anyone who has the public key can decrypt the bit sequence and thus verify the authenticity of this fingerprint or signature.

The usage of a certification authority means it is not necessary for each owner of a key to know every other owner. It is enough for them to know the certification authority. The additional information about the key further simplifies the administration of the key.

X.509 certificates are used, e.g. for e-mail encryption, in S/MIME or IPsec.

► **Client / Server**

In a client-server environment, a server is a program or computer, which accepts and answers queries from client programs or computers.

In data communication, a computer which establishes a connection to a server (or host) is also called a client. In other words, the client is the calling computer and the server (or host) is the computer called.

► **Datagram**

In the TCP/IP protocol, data is sent in the form of data packets, which are known as IP datagrams. An IP datagram has the following structure:

IP-Header	TCP, UDP, ESP etc. Header	Daten (Payload)
-----------	------------------------------	-----------------

The IP header contains:

- the IP address of the sender (source IP address)
- the IP address of the receiver (destination IP address)
- the protocol number of the protocol of the next higher protocol layer (in accord with OSI [seven layer] model)
- the IP header checksum used to check the integrity of the received header.

The TCP/UDP header contains the following information:

- the sender's port (source port)
- the recipient's port (destination port)
- a checksum covering the TCP header and some information from the IP header (among others the source and destination IP addresses)

► **DynamicDNS provider**

Every computer, which is connected to the Internet, has an IP address (IP = Internet Protocol). An IP address consists of a maximum of 4 three-digit numbers, which are each separated by a dot. If the computer accesses its Internet Service Provider (ISP) via a modem on a phone line, ISDN or ADSL, its ISP will assign it a dynamic IP address. In other words, it will be assigned a different address for every online session. If the computer is online 24 hours a day without interruption (e.g. in the case of a flat rate access), the IP address will even change during the session.

If a local computer should be accessible via the Internet, it must have an address that is known to the remote system. Unless this is true, no connection can be established between the remote system and the local computer. If the local computer's address is constantly changing, no connection can be setup. Unless, of course, the operator of the local computer has an account with a Dynamic DNS provider (DNS = Domain Name Server).

In this case, he/she can define a domain name in URL format (URL - Uniform Resource Locator) at this Dynamic DNS provider under which com-

puter should be accessible in the future, e.g.: www.xyz.abc.de. The Dynamic DNS provider also supplies a small program, which must be installed and run on this local computer. At each new Internet session, this tool will inform the Dynamic DNS provider which IP address the local computer has currently been assigned. This Domain Name Server will register the current assignment of Domain Name « IP Address and will also inform the other Domain Name Servers in the Internet.

If a remote system now attempts to establish a connection the local computer, which is register with the DynamicDNS provider, the remote system can use the host name of the local system as its address. This will setup a connection to the responsible DNS (Domain Name Server) to lookup the IP address that is currently registered for this domain name. The corresponding IP address will now be sent back from the DNS to the remote system, which can then use this as the destination address. The remote system can now directly address the desired local computer.

In principle, all Internet addresses are based on this procedure: First, a connection will be established to a DNS to lookup the IP address assigned for the domain name. Once that has been accomplished, this "looked up" IP address will be used to setup a connection the desired remote site, which could be any site in the Internet.

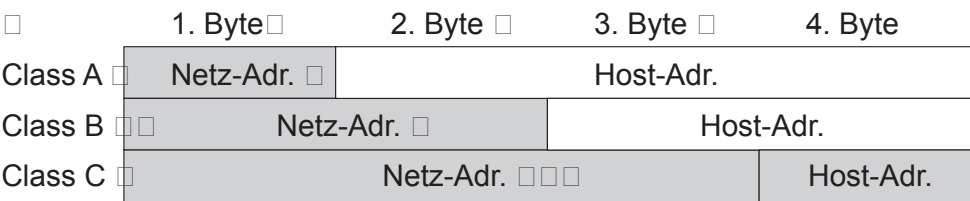
► **IP address**

Every host or router in the Internet or an Intranet has a unambiguous IP address (IP = Internet Protocol). The IP address is 32 bits (= 4 bytes) long and is written as 4 three-digit numbers (each in the range from 0 to 255), which are separated by a dot.

An IP address consists of 2 parts: the network address and the host address.

Network address	Host address
-----------------	--------------

Each host [or workstation] in a network has the same network address, but a different host address. Depending on the size of the respective network - networks are categorized as Class A, B or C networks, which are each different in size - the two parts of the address differ in length:



Whether the IP address of a device in a network is Class A, B or C can be seen in the first byte of the IP address. The following has been specified:

	Wert des 1. Byte	Bytes für die Netz-Adresse	Bytes für die Host-Adresse
Class A	1-126	1	3
Class B	128-191	2	2
Class C	191-223	3	1

As you can see, there can be a worldwide total of 126 Class A networks and each of these networks can have a maximum of $256 \times 256 \times 256$ hosts (3 bytes of address space). There can be 64×256 Class B networks and each of these networks can have up to $65,536$ hosts (2 bytes address space: 256×256). There can be $32 \times 256 \times 256$ Class C networks and each of these networks can have up to 256 hosts (1 bytes address space).

Subnet Mask see [“Subnet Mask” on page 201](#).

► IPsec

IP Security (IPsec) is a standard, which uses encryption to verify the authenticity of the sender and ensure the confidentiality and integrity of the data in IP datagrams (→ Datagram, [page 197](#)). The components of IPsec are the Authentication Header (AH), the Encapsulating Security Payload (ESP), the Security Association (SA) and the Internet Key Exchange (IKE).

To begin communication, the computers at both ends negotiate the mode to be used: `Transport Mode` or `Tunnel Mode`.

In `Transport Mode`, an IPsec header will be inserted between the IP header and the TCP or UDP header in each IP datagram. Since the IP header remains unchanged, this mode is only suitable for a host-to-host connection.

In `Tunnel Mode`, an IPsec header and a new IP header will be added in front of the entire IP datagram. As a consequence, the original datagram will be encrypted in its entirety and sent as the payload of the new datagram.

The Tunnel Mode is used in VPN applications: The devices at the tunnel ends ensure that the datagrams are encrypted before they pass through the tunnel so the actual datagrams are completely protected while being transferred over the public network.

► **NAT (Network Address Translation)**

Using Network Address Translation (NAT) – which is also often called IP-Masquerading – an entire network is “hidden” behind a single device, which is known as a NAT router. The internal computers in the local network with their IP addresses will remain hidden, if you communicate with the outside via a NAT router. The remote system outside will only see the NAT router with its own IP address.

If the internal computers are to directly communicate with external systems (in the Internet), the NAT router must modify the IP datagrams that are passed back-and-forth between the internal computers and the remote sites.

If an IP datagram is sent from the internal network to a remote site, the NAT router will modify the IP and TCP headers of the outgoing datagrams. It replaces the source IP address and port with its own official IP address and its - thus far unused - port. It maintains a table in which the original values listed together with the corresponding new ones.

When a reply datagram is received, the NAT router will recognize that it is actually for an internal computer from the datagram's destination port. Using the table, the NAT router will replace the destination IP address and port and pass the datagram on via the internal network.

► **Port Number**

The `Port Number` field is a 2 byte field in the UDP and TCP header. Port Numbers are used to identify the various data streams that are processed simultaneously by the UDP/TCP. The entire exchange of data between the UDP/TCP and the application processes is regulated via port numbers. The assignment of the port numbers to the application processes is dynamic and random. Fixed port numbers are assigned for certain, frequently used application processes. These are called "Assigned Numbers".

► **PPPoE**

The acronym for Point-to-Point Protocol over Ethernet. This protocol is based on the PPP and Ethernet standards. PPPoE defines how to connect users via Ethernet with the Internet via a jointly used broadband medium such as DSL, a Wireless LAN or a cable modem.

► **PPTP**

The acronym for Point-to-Point Tunneling Protocol. This protocol was developed in a cooperation between Microsoft, U.S. Robotics and others to securely transfer data between VPN nodes ([“VPN \(Virtual Private Network\)” on page 202](#)) via a public network.

► **Protocol, communication protocol**

Devices, which communicate with each other, must follow the same rules. They must "speak the same language". Such rules and standards are called protocols or communication protocols. Some of the more frequently used protocols include, for example, IP, TCP, PPP, HTTP and SMTP. TCP/IP is the general term for all protocols based on IP.

► **Service Provider**

Service providers are companies or institutions, which offer users access to Internet or an online service.

► **Spoofing, Anti-Spoofing**

In Internet terminology, spoofing means supplying a false address. With the false Internet address, the user can create the illusion of being an authorized user.

Anti-Spoofing is term for mechanisms, which detect or prevent spoofing.

► **Subnet Mask**

Normally, a company's network - with access to the Internet - is only officially assigned a single IP address, e.g. 134.76.0.0. Based on the first byte of this sample address, one can see that this company network is a Class B network and therefore the last 2 bytes are free to be used for host addresses. With a Class B network, the company network has address space for up to 65,536 hosts (256 x 256).

Obviously, such huge network is not practical. At this point, one can see a need for subnetworks. The standard answers this need with the Subnet Mask. Like an IP address, this mask is 4 bytes long. The bytes, which represent the network address, are each assigned the value 255. The main purpose of the mask is to "borrow" a portion of the host address which can then be used to address the subnetworks. As an example, by using the subnet mask 255.255.255.0 in a Class B network (2 bytes for the network address, 2 bytes for the host address), the third byte, which was actually intended for host addressing, can now be used for subnet addressing. With this configuration, the company's network could support 256 subnetworks that each have 256 hosts.

► **Symmetrical encryption**

In the case of symmetrical encryption, the same key is used to encrypt and decrypt the data. Two examples of symmetrical encryption algorithms are DES and AES. They are fast, but as the number of users increases the administration becomes rather involved.

► **TCP/IP** (Transmission Control Protocol/Internet Protocol)

This is a network protocol. It is used to connect two computers in the Internet.

IP ist das Basisprotokoll.

UDP is based on IP and sends individual packets. The packets may arrive at the recipient in an order different from that in which they were sent or they may even be lost.

TCP secures the connection and ensures, for example, that data packets are passed on the application in the right order.

UDP and TCP add the Port Numbers 1 to 65535 to the IP addresses. The various services offered by the protocols may be distinguished by these Port Numbers.

A number of additional protocols are based on UDP and TCP, e.g. HTTP (HyperText Transfer Protocol), HTTPS (Secure HyperText Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol, Version 3) and DNS (Domain Name Service)..

ICMP is based on IP and adds control messages.

UDP is based on IP and sends individual packets.

SMTP is an e-mail protocol that is based on TCP.

IKE is an IPsec protocol that is based on UDP.

ESP is an IPsec protocol that is based on IP.

On a Windows PC, the WINSOCK.DLL (or WSOCK32.DLL) handles both protocols.

(see datagram, [page 197](#))

► **VPN** (Virtual Private Network)

A Virtual Private Network (VPN) connects several separate private networks (subnets) together via a public network, e.g. the Internet, to form a single joint network. A cryptographic protocol is used to ensure confidentiality and authenticity. A VPN thus offers an economical alternative to using dedicated lines to build a nationwide corporate network.

C Reader's comments

What is your opinion of this manual? We are always striving to provide as comprehensive a description of our product as possible, as well as important information that will ensure trouble-free operation. Your comments and suggestions help us to further improve the quality of our documentation.

Your **assessment** of this manual:

	excellent	good	satisfactory	mediocre	poor
Accuracy	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Readability	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Comprehensibility	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Examples	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Structure/Layout	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Completeness	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Graphics	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Drawings	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tables	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Did you discover an error in the manual?
If so, on what page?

.....

.....

.....

.....

.....

.....

.....

Suggestions for improvement and additional information:

.....

.....

.....

.....

General comments:

.....

.....

.....

.....

Company / Department

Name / Telephone number

Street

Zip code / City

Date / Signature

Dear User,

Please fill out and return this page

- by fax to the number +49 (0)7127/14-1798 or
- by mail to

Hirschmann Electronics GmbH & Co. KG
Department AMM
Stuttgarter Str. 45- 51

72654 Neckartenzlingen
Germany

D Index

Numerics

1-to-1 NAT	19
3DES	105, 195
3DES-168	106

A

ACA	34, 134
Administration	118
Administrator interface	137
Administrator password	29
Administrators	155
ADSL	197
AES	97, 195
AES-256	106
Agent alarm	134
AH	199
Air humidity	8
Air temperature	8
Alarm	133
American National Bureau of Standard	195
Anti-Spoofing	201
Assigned Numbers	200
Asymmetrical encryption	195
Authentication	104, 146
Authentication Header	199
Authenticity	196, 199, 202
Authorization level	136
Auto Configuration Adapter	34, 134
Automatic Configuration	64
Autonegotiation	33

B

Browser	53, 138
---------	---------

C

CA	196
Cache	45
CANopen	68
CE	10
Certification Authority	196
Chassis alarm	134
Checksum	197
Checksum algorithm	106
CIDR 69, 85, 87, 92, 140, 143, 146, 149, 160	
Class A	198
Client 19, 21, 22, 107, 123, 125, 197	
Climatic	8
Communication protocol	201
Configuration	41, 64
Configuration setting	156

Cryptographic protocol	202
------------------------	-----

D

Datagram	104
DES	146, 195
Destination IP address	197, 200
Destination NA	88
Destination port	197
DHCP 73, 76, 80, 118, 123, 125, 134, 173	
DHCP client	123, 125
DHCP server 134, 168, 170, 172, 173	
Digital signature	195, 196
Distinguished Name	196
DN	196
DNS 117, 197, 198, 202	
Domain address	117
Domain name 120, 197	
Domain nameserver	117
Domain suffix	118
DSL	200
Dynamic DNS provider	197
Dynamic IP address	197
DynamicDNS	197
DynDNS Login	122
DynDNS Password	122
DynDNS server 120, 122, 158	
DynDNS Service	100

E

Electromagnetic compatibility	10
EMC	10
Encapsulating Security Payload	199
Encryption	195, 199
ESP	199, 202
ESP-Header	197
EU conformity declaration	10

F

Factory setting	42, 91
FCC	11
Fingerprint	196
Firewall	43, 83
Firmware	165
Flat rate	197
Forward	89

G

Gateway	100, 115, 158
Ground	8, 32
Ground cable	35

- Ground screw 35
- H**
- Hardware 155
- Hash 106, 196
- Hash algorithms 97
- HCP server 124, 126
- Header 88
- HiDiscovery 39, 61
- Host address 198, 201
- Hostname 118
- Hostname mode 118
- HTTP 137
- HTTPS 42, 47, 202
- HTTPS login 134
- HTTPS Remote Access 139, 158
- I**
- IANA 85
- ICMP 85, 87, 202
- IKE 199, 202
- Indicator contact 25
- Internet Key Exchange 199
- Internet Service Provider 78, 79, 100, 120
- IP 85, 87, 202
- IP address 100, 198
- IP datagram 197
- IP header 199
- IP masquerading 90
- IP Security 199
- IP-Header 197
- IP-Masquerading 200
- IPsec 97, 105, 114, 195, 196, 199
- IPsec connection 97
- IPsec header 199
- IPsec Status 115
- ISAKMP 106, 115
- ISDN 197
- ISP 78, 79, 120, 197
- K**
- Key exchange 106
- L**
- L2TP 102, 107
- L2TP status 116
- Language 138, 159
- Language setting 138
- Link Layer Discovery Protocol 128
- Linux 173
- LLDP 128
- Local configuration 41
- Login 44, 78, 79, 118
- M**
- Main Mode 97
- MARS 196
- MD5 97, 106, 146
- Modem 48, 197
- Modem cable 35
- Monitoring proper functioning 62
- MS Internet Explorer 43
- N**
- NAT 19, 90, 97, 200
- NAT router 97, 200
- National Institute of Standards and Technology 195
- NAT-T 97
- Netmask 108
- Network address 198, 201
- Network Address Translation 90, 200
- Network mask 73, 107
- Network Time Protocol 129
- NIST 195
- Norms 185
- NSA 195
- NTP 129
- O**
- Online service 201
- Operating mode 64
- Operating system 169
- P**
- Password 44, 78, 79, 146
- PELV 7
- Perfect Forward Secrecy 107
- PFS 102, 107
- Phone line 197
- Phone number 49
- Point-to-Point Protocol 200
- Point-to-Point Tunneling Protocol 200
- Pollution Degree 8
- POP3 85, 87, 202
- Port number 47, 85, 140, 200
- Power Supply 134
- PPP 102, 200
- PPP connection 114
- PPPoE 157, 200
- PPPoE Login 78, 79
- PPPoE mode 73, 91
- PPPoE Password 78, 79
- PPTP 157, 200
- Pre-Shared Key 104, 105
- Private Key 195
- Private network 202
- Profile 56

Protocol	201	Signature	196
Provider	73, 118	Simple Network Management Protocol	145
Provider defined	118	SMTP	202
Proxy server	43	Snap-in guide	31
PSK	105	Snapshot.tar.gz	156
Public Key	104, 195, 196	SNMP	145
Public network	202	Software module	154
		Software version	159
		Source IP address	197
		Source port	197
		Spoofing	201
		SSH	118, 136
		SSH remote access	142, 158
		SSL	42, 47
		Standard gateway	73
		Standards	185
		State on delivery	136, 169
		Stateful Packet Inspection	83
		Stealth mode	100
		Subnet	201, 202
		Subnet mask	123, 125, 201
		Subnetwork	124, 126
		Supply voltage	7, 24, 25, 30
		Support	155
		Surrounding air temperature	8
		Symmetrical encryption	195
		System time	129
		System update	152
		System Uptime	159
		T	
		TCP	85, 87, 202
		TCP header	199, 200
		TCP/IP	53, 127, 197
		TCP-Header	197
		Telephone network	48
		Temperature	8, 134
		Terminal block	31
		Terminal cable	35
		TFTP	173
		TFTP server	168, 170, 172, 173
		TFTP service	173
		Traffic	115
		Transparent	85, 87, 110, 141, 144, 150, 157
		Transparent mode	85, 87
		Transport Mode	199
		Trap	133
		Tunnel Mode	199
		Tunnels	105
		Twofish	196
		U	
		UDP	85, 87, 200, 202
		UDP header	197, 199
Q			
Quick Mode	97		
R			
RC6	196		
Reboot	152		
Recovery	27		
Recovery button	168		
Recovery procedure	165		
Recovery status	168		
Recovery switch	165		
Recycling	11		
Redundant power supply	62		
Refresh Interval	122		
Relay contact	62		
Remote configuration	41		
Remove	36		
Restart	166, 167		
RFC 1518	160		
Rijndael	196		
Root	136		
Root password	29, 136		
Router	157, 198		
Router mode	73		
RSA	195		
S			
S/MIME	196		
SA	199		
SA Lifetime	97		
Safety certificates	97		
Safety regulations	9		
SDO	68		
Security	134		
Security Association	199		
Security notice	44		
SELV	7		
Serpent	196		
Server	197		
Service Data Object	68		
Service names	85		
Service Provider	201		
SHA-1	97, 106		
Shell login	134		
Shielding ground	7		
Signal contact	30, 62		

Update	152
URL	197
User defined	118
User name	44, 78, 79
User password	137

V

V.24 interface	34
V.24 port	48
Virtual Private Network	202
VLAN	74
VLAN ID	74
VPN	200, 202
VPN application	199
VPN client	19
VPN connection	83, 91, 97, 120, 158
VT100	34

W

WAN	47, 73, 157
Web browser	42, 47, 140
Windows system	171
Wireless	200

X

X.509	104, 196
-------	----------

Hirschmann Competence

In the longterm, product excellence alone is not an absolute guarantee of a successful project implementation. Comprehensive service makes a difference worldwide. In the current scenario of global competition, the Hirschmann Competence Center stands head and shoulders above the competition with its comprehensive spectrum of innovative services:

- ▶ Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- ▶ Training offers you an introduction to the technological fundamentals, product briefing and user training with certification.
- ▶ Support ranges from commissioning through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you firmly rule out any compromise: the client-specific package leaves you free to choose the service components that you will use.

Internet:

<http://www.hicomcenter.com>

